POHJOIS-KARJALAN AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma

Leevi Hertteli

TYÖPÖYTÄ/SOVELLUSVIRTUALISOINNIN OPETUSYMPÄRISTÖN SUUNNITTELU JA RAKENTAMINEN

Opinnäytetyö
Helmikuu/2011

NORTH KARELIA
UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ
Helmikuu 2011
Tietotekniikan koulutusohjelma

Karjalankatu 3
80200 JOENSUU
p. (013) 260 6800 p. (013) 260 6801

Tekijä
Leevi Hertteli

Nimeke
Työpöytä/Sovellusvirtualisoinnin opetusympäristön suunnittelu ja rakentaminen

Toimeksiantaja
Pohjois-Karjalan AMK

Yritykset ovat yhä enenevässä määrin kiinnostuneita siirtämään IT-toimintojaan virtuaalisiksi teknologioiksi muun muassa kustannusäästöjen ja joustavamman tietohallinnon vuoksi. Virtualisoinnin osa-alueista palvelinvirtualisointia on hyödynnetty jo useita vuosia. Työpöytä- ja sovellusvirtualisoinnin käyttö on jatkuvasti lisääntymässä.

Opinnäytetyön tavoitteena oli laatia havainnollinen tietopaketti virtualisoinnista ja selvittää, mihin käyttötarkoituksiin työpöytä- ja sovellusvirtualisointia voitaisiin soveltaa opetusympäristössä. Työssä tehtiin testiympäristöt markkinoiden kärkituotteilla, jotka ovat Microsoft Remote Desktop Services ja VMware View. Kaikki asennukset dokumentoitiin.

Kummassakin testiympäristössä käytettiin samaa HP-palvelinta, johon asennettiin virtualisointialustaksi VMware ESXi 4.1. HP-palvelimelle luotiin useita virtuaalipalvelimia, joihin asennettiin Windows Server 2008 R2 käyttöjärjestelmä ja etäpöytäpalveluun vaadittavat komponentit.

Microsoftin tuotteella tehtiin kokoonpanoltaan ja toiminnaltaan kattavampi testiympäristö kuin VMwarella. Microsoftin testiympäristöön sisällytettiin terminaalipalveluun ja sovellusten etäkäyttöön liittyviä ominaisuuksia. VMwaren toteutuksessa kokeiltiin työpöytävirtualisointia. Etäpöytäjärjestelmiä testattiin sisä- ja ulkoverkon työasemilta internetselaimen tai Windowsin oman etäpöytäsovelluksen kautta. Molemmilla tuotteilla onnistuttiin toteuttamaan työpöytä- ja sovellusvirtualisointiympäristöt, joita voidaan hyödyntää oppimisympäristön luomisessa.

Kieli
suomi

Sivuja 45
Liitteet 4
Liitesivumäärä 56

Asiasanat
virtualisointi, työpöytävirtualisointi, sovellusvirtualisointi

NORTH KARELIA
UNIVERSITY OF APPLIED SCIENCES

THESIS
February 2011
Degree programme in
InformationTechnology
Karjalankatu 3
FIN 80200 JOENSUU
FINLAND
Tel. 358-13-260 6800

Author
Leevi Hertteli

Title
Planning and Installing of a Teaching Environment for Desktop/Application Virtualization

Commissioned by
North Karelia University

Enterprises are more and more interested in transforming their IT-operations into virtualized technologies, because of cost saving and more flexible data administration. Server virtualization has been utilized for several years and the use of desktop and application virtualization is constantly increasing.

The purpose of this study was to compile an illustrative information package of virtualization and to clarify in which uses desktop and application virtualization could be applied in a learning environment. In this study, test environments were constructed by using the leading products in the market, Microsoft Remote Desktop Services and VMware View. All the installations were documented.

The same HP-server was used in both of the test environments. VMware ESXi 4.1 was installed as virtualization platform. Several virtual machines were created to the HP-server and they were equipped with Windows Server 2008 R2 operating system and with the components needed for remote desktop services.

The test environment created by the Microsoft's product was more extensive for its assembly and operation than the environment created by the VMware's product. Features concerning Terminal Services and remote use of applications were included in the test environment of Microsoft. Desktop virtualization was used in the test environment of VMware. Remote Desktop Systems were tested through internet browser or the remote desktop software of Windows by using internal and external desktops. Desktop and application environments were successfully created and they can be further utilized in creating a learning environment.

Language	Pages 45
Finnish	Appendices 4
	Pages of Appendices 56

Keywords

virtualization, desktop virtualization, application virtualization

SISÄLLYSLUETTELO

1 JOHDANTO 7
1.1 Työn tavoite 7
1.2 Rajaukset 7
1.3 Työympäristö 8
2 VIRTUALISOINTI 8
2.1 Virtualisoinnin määritelmä 9
2.2 Virtuaaliympäristön arkkitehtuuri 10
2.3 Virtualisointiratkaisut 11
2.3.1 Palvelinvirtualisointi 12
2.3.2 Sovellusvirtualisointi 12
2.3.3 Työpöytävirtualisointi 13
2.3.4 Esityskerrosvirtualisointi 13
2.4 Virtualisointiin ajavat tekijät ja sen tuomat hyödyt 13
2.5 Virtualisoinnin hyödyntäminen opetusympäristössä 15
3 MICROSOFTIN VIRTUALISOINTIRATKAISU 16
3.1 Remote Desktop Services -roolit 16
3.2 Remote Desktop Services -lisenssit 18
3.3 Laitevaatimukset 20
4 VMWAREN VIRTUALISOINTIRATKAISU 21
4.1 VMware View 21
4.2 Laitevaatimukset 27
4.3 Lisenssit 28
5 SUUNNITTELU 29
6 TESTIYMPÄRISTÖJEN TESTAUS 33
6.1 Microsoft RDS testaus 34
6.2 VMware View testaus 39
7 POHDINTA 41
LÄHTEET 44

LIITTEET
Liite 1: Microsoft RDS -testiympäristön asennusohje
Liite 2: VMware View 4.5 -testiympäristön asennusohje
Liite 3: Reitittimen konfiguraatio
Liite 4: Kytkimen konfiguraatio

LYHENTEET

AD	Active Directory on Microsoftin käyttäjätietokanta ja hakemistopalvelu, joka sisältää tietoja tietokoneista, käyttäjistä ja verkon resursseista.
CAL	Client Access License, asiakkaan käyttöoikeuslisenssi käyttäjille, joilla on käyttöoikeus palvelinohjelmistoihin.
DC	Domain Controller, ohjauskone toimii NT- tai Active Directory -toimialueen ylläpitäjänä. Sen päätarkoituksena on ylläpitää tietokantaa toimialueen resursseista ja tunnistaa toimialueelle kirjautuvat käyttäjät.
DHCP	Dynamic Host Configuration Protocol on verkkoprotokolla, jonka tarkoituksena on jakaa IP-osoitteita lähiverkkoon kytkeytyville laitteille.
DMZ	Demilitarized zone, tarkoittaa fyysistä tai loogista aliverkkoa, joka liitetään organisaation oman järjestelmän ulkopuolelle, jolla lisätään turvatasoa.
DNS	Domain Name System on verkkoympäristöissä nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.
HTTPS	Hypertext Transfer Protocol Secure, http:n salattu versio, jota käytetään webissä siirrettävissä tiedoissa käyttäen SSL-protokollaa.
Hyper-V	Microsoft:n virtualisointijärjestelmä, jolla voidaan luoda virtuaalikoneita.
PcoIP	PC-over-IP, Teradicin patentoima protokolla, joka mahdollistaa etäpääsyn työasemille ja palvelimille.
RD CAP	Remote Desktop Connection Authorization Policy, etäpöytäyhteyden auktorisointikäytäntö.
RD RAP	Remote Desktop Resource Authorization Policy, etäpöytäresurssien auktorisointikäytäntö.

RD	Remote Desktop, jota käytetään lyhenteenä Remote Desktop Services -roolien nimissä.
RDC	Remote Desktop Connection, Microsoftin kehittämä etätyöpöytäyhteys-protokolla, jota käytetään etäpöytäjärjestelmän asiakaskoneissa.
RDP	Remote Display Protocol, Windows:n graafinen etäkäyttöprotokolla.
RDS	Remote Desktop Services, Microsoftin virtualisointiratkaisu.
RemoteApp	
RGS	Remote Graphics Software, Hewlett-Packard kehittämä etäkäyttöprotokolla, joka mahdollistaa etäpääsyn huipputehokkaisiin työasemiin kevytpäätteiltä.
RQDN	Fully Qualified Domain Name on domain-nimi, joka määrittelee tarkan sijainnin DNS-hierarkiassa.
sign-on	Kertakirjautuminen on menetelmä, jossa pääsy palveluihin toteutetaan yhdellä käyttäjän autentikonnilla.
SSL	Secure Sockets Layer on salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.
Thin client	Kevyt asiakaspääte on riisuttu tietokone, jonka tarkoituksena on toimia yhteydenpitovälineenä tehokkaampaan keskustietokoneeseen.
VDI	Virtual Desktop Infrastructure, virtuaalinen työpöytä on verkossa oleva, työasemariippumaton, käyttäjän tarpeisiin mukautettu työpöytä.
VLAN	Virtual VLAN on tekniikka, jolla fyysinen tietoliikenneverkko voidaan jakaa loogisiin segmentteihin.
VPN	Virtual Private Network on tapa, jolla useiden yritysten verkkoja voidaan yhdistää julkisen verkon yli muodostamalla näennäisesti yksityinen verkko.

1 JOHDANTO

Yritykset ovat yhä enenevässä määrin kiinnostuneita siirtämään IT-toimintojaan virtuaalisiksi teknologioksi. Yleisen talouden heikkeneminen on ollut osaltaan vaikuttamassa virtualisoinnin voimakkaampaan esiintuloon kustannussäästöjen vuoksi. Virtualisoinnin osa-alueista palvelinvirtualisointia on hyödynnetty jo useita vuosia. Työpöytä- ja sovellusvirtualisoinnin käyttö on jatkuvasti lisääntymässä. Opinnäytetyössä perehdytään virtualisoinnin tietoviidakkoon ja suunnitellaan sekä rakennetaan testiympäristöt VMwaren ja Microsoftin tuotteilla opetusympäristötarkoituksiin.

1.1 Työn tavoite

Opinnäytetyön tavoitteena on laatia havainnollinen tietopaketti virtualisoinnista ja selvittää, mihin käyttötarkoituksiin työpöytä- ja sovellusvirtualisointia voitaisiin soveltaa opetusympäristössä. Työssä tehdään testiympäristöt markkinoiden kärkituotteilla. Toteutettujen ympäristöjen vertailun pohjalta tehdään työpöytäympäristö (VDI), joka tarjotaan palveluna opiskelijaryhmille. Kaikki testiympäristöön tehdyt asennukset dokumentoidaan kuvineen.

1.2 Rajaukset

Työssä tutustutaan markkinoiden kärkivalmistajien (Microsoft, VMware) tarjoamiin työpöytä- ja sovellusvirtualisoinnin ratkaisuihin sekä perehdytään virtualisointiin liittyviin menetelmiin. Microsoftin ja VMwaren ratkaisuilla rakennetaan

testiympäristöt ilmais- ja demoversioita käyttäen. Kärkivalmistajiin lukeutuisi myös Citrixin tarjoama ratkaisu, mutta se rajataan tämän opinnäytetyön ulkopuolelle.

1.3 Työympäristö

Opinnäytetyö suoritetaan Pohjois-Karjalan ammattikorkeakoulun Wärtsilän toimipisteen tietotekniikan laboratoriossa. Wärtsilän kampuksella opiskelee noin 1400 liiketalouden ja tekniikan opiskelijaa. Wärtsilä-keskus on alueensa kehittäjä, kansallisesti ja kansainvälisesti merkittävä opiskelijoiden, henkilöstön ja työelämäkumppaneiden koulutus-, oppimis- ja kehittämisyhteisö. Keskuksessa tarjotaan opetusta kuudessa eri AMK-tutkintoon ja yhdessä ylempään AMK-tutkintoon johtavassa koulutusohjelmassa. Teknologia-osaamisen johtamisen koulutusohjelmasta valmistutaan nimikkeellä insinööri (ylempi AMK, Master of Engineering), liiketalouden opinnoista tradenomiksi ja muista koulutusohjelmista saadaan tutkintonimike insinööri (AMK).

2 VIRTUALISOINTI

Nykypäivän muotisanaksi tietotekniikassa on muodostunut sana virtualisointi, josta on tullut IT-alalla trendi ja tulevaisuudessa on myös tavallisten kuluttajien käyttämä termi. Virtualisointi parantaa fyysisten laitteiden käyttöastetta, nopeuttaa niiden käyttöönottoa, säästää tilaa palvelinhuoneessa, laskee virrankulutusta, nopeuttaa ongelmatilanteista toipumista ja tuo tietohallintoon joustavuutta.

Vaikka virtualisointi on nykyaikaa, niin se ei ole tämän vuosituhannen keksintö. Virtualisointi on tunnettu jo 1960-luvulta lähtien, jolloin sitä kutsuttiin nimellä

“Time sharing”. Virtualisoinnin keksijänä pidetään Oxfordin yliopiston professoria Christopher Stracheytä. (Ditter & Rule 2007, 32.)

Stracheytin keksimää menetelmää käytettiin ensimmäisen kerran 1960-luvun alkupuolella “The Atlas Computer” nimiseen supertietokoneeseen. Kyseisessä supertietokoneessa pystyttiin suorittamaan seuraavia toimintoja: moniajoa ja jaettua oheislaitteiden käyttöä. (Dittner & Rule 2007, 32.)

Toisena merkittävänä hankkeena virtualisoinnin alkuaikoina pidetään IBM:n M44/44x-projektia. Projektissa luotiin samankaltainen arkkitehtuuri kuin “The Atlas Computerissa”. Kehitysprojektin tuloksena pystyttiin ajamaan M44/44X-tietokoneella monia simuloituja virtuaalikoneita käyttämällä hyödyksi isäntäkoneen laitteistoa, ohjelmistoa, muistia ja moniajoa. (Dittner ja Rule 2007, 32.)

1980-luvun ja 1990-luvun välisenä aikana pöytätietokoneet ja x86-palvelimet tulivat markkinoille ja virtualisointiteknologian kehitystyö loppui. Windows ja Linux -tuotteiden kehittyminen johti laitteistojen ja sovellusten halpenemiseen, jolloin virtualisoinnin tarpeellisuus jäi vähäisemmäksi. (VMware 2011a.)

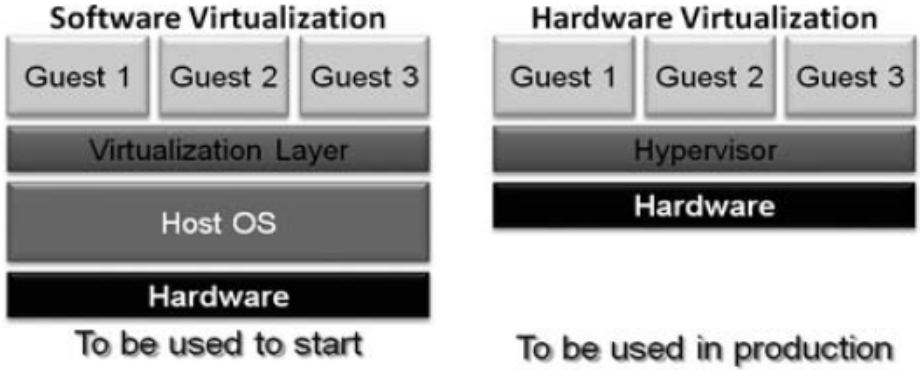
Virtualisointi kuitenkin näki päivänvalon, kun VMware kehitti x86-järjestelmille tarkoitetun virtualisointialustan vuonna 1999. Siitä lähtien virtualisoinnin kehittäminen on ollut nousujohteista. Nykyään VMware on virtualisointi-ratkaisujen tuottajana markkinajohtaja. (VMware 2011a.)

2.1 Virtualisoinnin määritelmä

Virtualisointiteknologialla mahdollistetaan yksittäisen fyysisen resurssin kuten palvelimen, käyttöjärjestelmän, sovelluksen tai tallennuslaitteen näyttäytyminen monina loogisina resursseina tai vastaavasti monien fyysisten resurssien kuten tallennuslaitteiden tai palvelimien näyttäytyminen yhtenä loogisena resurssina. (Bolton 2011.)

2.2 Virtuaaliympäristön arkkitehtuuri

Virtualisointiympäristöjä on rakenteeltaan kahdenmallisia, ohjelmisto- ja rautapohjaista ratkaisuja (kuva 1). Ohjelmistopohjaista käytetään pääosin testi- ja kehitysympäristöissä. Tässä ratkaisussa tarvitaan erikseen virtuaalikerroksen alle isäntäkäyttöjärjestelmä. Rautapohjaisessa ratkaisussa ei tarvita isäntäkäyttöjärjestelmää, koska virtuaalikerrokseksi kutsuttu hyper-V (hypervisor) kykenee välittämään itse fyysisen laitteen resursseja virtuaalikoneille. Rautapohjainen ratkaisu on paras tuotantoympäristökäytössä tehokkuutensa vuoksi. Näiden palvelinvirtualisoinnin eri ratkaisujen osia selitetään tarkemmin alla. (Ruest & Ruest 2009, 33.)



Kuva 1. Virtualisointiympäristön ohjelmisto- ja rautapohjaiset mallit. (Ruest & Ruest 2009, 33.)

Isäntäkone

Isäntäkoneeksi (host machine) kutsutaan virtuaaliympäristössä fyysistä palvelinta, johon virtualisointijärjestelmä on asennettu ja joka ylläpitää palvelimelle asennettuja virtuaalikoneita. (Desai 2007, 4)

Isäntäkäyttöjärjestelmä

Isäntäkäyttöjärjestelmä (Host OS) on pääkäyttöjärjestelmä palvelimessa, johon on asennettu virtualisointijärjestelmä. Isäntäkäyttöjärjestelmällä on suora yhteys alustalaitteelle ja se sisältää laiteajurit, joita se voi välittää järjestelmään liitettäville laitteille. Ohjelmistopohjaisessa mallissa virtuaalikerroksen ja laitteiston väliin vaaditaan isäntäkäyttöjärjestelmä. (Desai 2007, 4)

Virtualisointikerros

Virtualisointikerros on vastuussa optimaalisesta resurssien jaosta kaikkiin virtuaaliympäristön koneisiin. Se toimii väylänä kaikilta virtuaalikoneilta isäntäkoneen resursseihin.

Virtuaalikone

Virtuaalikone on virtuaalinen versio fyysisestä palvelimesta tai työasemasta. Virtuaalikone toimii omana palvelimenaan riippumatta muista isäntäkoneelle asennetuista virtuaalikoneista. Niitä voidaan luoda fyysiseen palvelimeen asennettavalla virtualisointijärjestelmällä kuten VMware ESX. Virtuaalikoneet käyttävät fyysisen palvelimen resursseja (muistia, tallennustilaa, prosessoria). (Wiki, 2011.)

Vieraskäyttöjärjestelmä

Virtuaalikoneeseen asennettavaa käyttöjärjestelmää kutsutaan vieraskäyttöjärjestelmäksi (Guest operating system).

2.3 Virtualisointiratkaisut

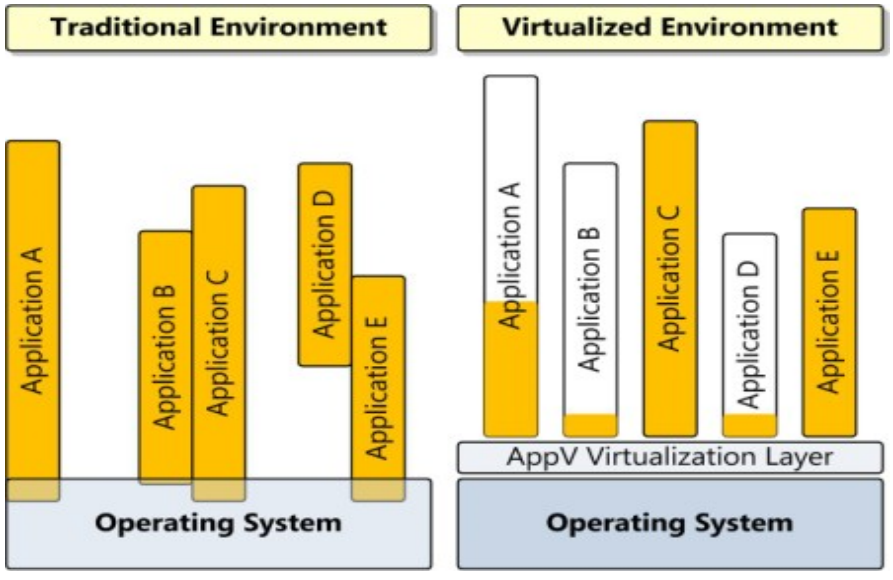
Virtualisointia voidaan hyödyntää moniin käyttötarkoituksiin. Tässä luvussa esitetään niitä virtualisointimenetelmiä, jotka keskeisesti liittyvät opinnäytetyön aiheeseen.

2.3.1 Palvelinvirtualisointi

Palvelinvirtualisointi on tähän mennessä ylivoimaisesti käytetyin virtualisointimenetelmä. Tällä virtualisointimenetelmällä yksittäiseen fyysiseen palvelimeen voidaan asentaa useita virtuaalipalvelimia. Kullekin virtuaalipalvelimelle voidaan asentaa erillinen käyttöjärjestelmä.

2.3.2 Sovellusvirtualisointi

Sovellusvirtualisoinnilla sovellusten välittäminen käyttäjille toteutuu omana palvelunaan. Tällöin sovellusten toiminta erotetaan kokonaan käyttöjärjestelmästä ja muista työasemassa ajettavista sovelluksista. Kuvassa 2 nähdään, kuinka sovellusten ajaminen tapahtuu ilman virtualisointia sekä virtualisoinnin kanssa. (Ruest, D. & Ruest, N. 2008.)



Kuva 2. Sovellusten toimintaperiaate perinteisessä ja virtualisoidussa ympäristössä. (Ruest, D. & Ruest, N. 2008)

2.3.3 Työpöytävirtualisointi

Työpöytävirtualisoinnilla järjestetään työpöytien käyttö virtuaalisena paikasta ja päätelaitteesta riippumatta keskitettynä palveluna, palvelinsalissa toimivalta palvelimelta. Palvelimen tarjoamaa työpöytää voidaan ajaa erityyppisillä päätelaitteilla kuten kevytpäätteillä, kotikoneilla tai julkisilla koneilla. Jaettavaan työpöytäinstanssiin voidaan asentaa jokin seuraavista käyttöjärjestelmistä: Windows XP, Windows Vista, Windows 7 tai Linux-versio. Nämä työpöytäinstanssit voidaan jakaa käyttäjille poolista tai nimetään käyttäjälle henkilökohtainen työpöytä. (Ruest & Ruest 2009, 39.)

2.3.4 Esityskerrosvirtualisointi

Esityskerrosvirtualisointi on perinteinen Terminal Server -ratkaisu. Se on vaihtoehtoinen tapa toimittaa työpöydät ja yksittäiset sovellukset palvelimelta loppukäyttäjille. Tämä virtualisointimenetelmä eroaa työpöytävirtualisoinnista siten, että käyttäjät, jotka ovat yhteydessä terminaalipalvelimeen, jakavat työpöytäympäristön keskenään. Työpöytävirtualisoinnissa jokaiselle käyttäjälle annetaan oma työpöytä, johon on asennettu jokin seuraavista käyttöjärjestelmistä: Windows XP, Windows 7, Windows Vista tai Linux-versio. (Ruest & Ruest 2009, 33.)

2.4 Virtualisointiin ajavat tekijät ja sen tuomat hyödyt

Virtualisoinnilla saadaan aikaiseksi merkittäviä parannuksia fyysisiin järjestelmiin nähden, vaikka kustannukset laskevat. Virtualisoinnilla sovitetaan tarpeisiin

nähden juuri sen verran resursseja, mitä toteutettava IT-ympäristö tarvitsee. Tällöin tuhlataan vähemmän resursseja. Skaalautuvuus, virtuaaliympäristön muokattavuus ja käytettävyys lukeutuvat myös merkittäviin etuihin. Virtualisoinnin tuomia etuja voidaan katsoa taulukossa 1 esiintyvien kustannuslaskelmien valossa, jossa verrataan fyysisen järjestelmän kustannuksia virtuaalijärjestelmän kustannuksiin. Virtuaalijärjestelmän kustannukset ovat noin viidesosa fyysisen järjestelmän kustannuksista.

Taulukko 1. Kustannuslaskelma fyysisestä- ja virtuaalisesta järjestelmästä. (Ditter & Rule 2007, 9.)

Component	Unit Cost	Physical Cost	Virtual Cost
Server hardware	$7,500.00	$37,500.00	$7,500.00
Software licenses/CPU	$2,000.00	$20,000.00	$4,000.00
Supporting infrastructure	$2,500.00	$12,500.00	$2,500.00
Power per server year	$180.00	$2,700.00	$540.00
Cooling per server year	$150.00	$2,250.00	$450.00
Total three-year costs:		$74,950.00	$16,490.00
Realized savings over three years:	$58,460.00		

Taloudellisten hyötyjen lisäksi virtualisointi on ympäristöystävällinen. Hiilijalanjälki pienenee laitteiden vähentymisen myötä, kun jäähdytykseen ja laitteisiin tarvittava energian määrä laskee. Säästetään rahaa ja palvelinsalissa tilaa. Virtualisoinnin merkittävimpinä hyötytekijöinä voidaan pitää työasemien hallintaa ja kulujen säästöä. (Atea 2011a.)

Päätelaitteiston fyysinen resurssi toimii palvelinpäässä, jossa myös säilytetään päätelaitteiston tallennuskapasiteetti. Eri ohjelmien ja uusien käyttöjärjestelmien asennusta vanhoille työasemille ei tarvitse miettiä, koska laitevaatimuksien tulee täyttyä vain etäpalveluja välittävässä palvelimessa. Ohjelmistopäivitysten tekeminen on vaivatonta, koska päivityksiä tarvitse tehdä vain yhteen paikkaan. Sama pätee myös tietoturvan ylläpitämisessä. (Atea 2011a.)

2.5 Virtualisoinnin hyödyntäminen opetusympäristössä

Virtualisoinnin soveltaminen opetusympäristössä monipuolistaa opetuksen toteuttamista. Suurissa oppimisinstituutioissa työasemia kertyy ja vanhoja työasemia saattaa jäädä käyttämättömiksi laitepäivitysten vuoksi. Virtualisoinnilla voidaan antaa uusi elämä vanhoille työasemille. Vanhojen työasemien hyödyntäminen etäpöytäpalveluiden päätetyöasemina on erittäin hyvä ratkaisu. Siten vanhojen työasemien käyttöaikaa voidaan pidentää. (Atea 2011a.)

Perinteisesti kouluissa tiettyihin kursseihin vaadittavat erityisohjelmat asennetaan yksittäisiin luokkatilojen tietokoneisiin, jotka on varustettu luokkalisenssillä. Näin ollen erityisohjelmien toimittaminen opiskelijoille rajoittuu luokkien varaustilanteiden vuoksi, mikä myös vaikeuttaa opiskelijoiden mahdollisuuksia tehdä opiskeluihinsa kuuluvia harjoituksia. Tämä johtaa myös siihen, että luokkaympäristöissä lisenssien hyöty minimoituu ja käyttöön on etsittävä kone, joka sisältää halutun ohjelmiston.

Virtualisointi mahdollistaa monien epäkohtien poistamisen. Virtuaalisella työpöytäratkaisulla kursseihin vaadittavat ohjelmistot voidaan jakaa palvelimelta juuri niille käyttäjille, jotka oikeasti tarvitsevat niitä. Ohjelmistojen ja tiedostojen käyttö mahdollistetaan paikasta ja laitteistosta riippumatta. Palvelimeen keskitetyt ohjelmat saadaan välitettyä käyttäjille profiiliasetuksineen myös koulun ulkopuolelle, kunhan päätelaite kytketään internetiin.

Uusien ohjelmien tai ohjelmistojen päivitykset tarvitsee tehdä vain palvelimelle, jossa kyseisiä ohjelmia ylläpidetään. Ajantasaiset ohjelmat saadaan välitettyä nopeasti käyttäjille. Kurssit muuttuvat vuosittain ja sitä mukaa kursseihin vaadittavat ohjelmat vaihtuvat. Uusien ohjelmien käyttöönotto nopeutuu keskitetyn hallinnan ansiosta. (Atea 2011b.)

Sovellusten välittäminen käyttäjille on yksi tärkeä opintoja tukeva tekijä. Sen lisäksi virtualisoinnin vieminen laboratorioympäristöön, jossa harjoitellaan eri käyttöjärjestelmiä, palvelinhallintaa ja monipalvelinympäristön ylläpitoa. Henkilökohtaisen palvelimen jakaminen virtuaalisesta ympäristöstä käyttäjille antaisi jokaiselle oppijalle konkreettisen oppimiskokemuksen palvelinhallintaan liittyvistä asioista. (Atea 2011a.)

3 MICROSOFTIN VIRTUALISOINTIRATKAISU

3.1 Remote Desktop Services -roolit

Microsoftin Remote Desktop Services sisältää kuusi erilaista roolia, joilla on oma tehtävä. Etäpöytäpalvelun pystyttämisessä ei välttämättä tarvitse ottaa kaikkia rooleja käyttöön. Roolien tarve riippuu rakennettavan etäpalvelun laajuudesta, etäpöytäpalvelun käytön tarpeesta sisäverkon ja ulkoverkon puolella.

Terminal services sisältää kuusi erilaista roolia, joiden nimet ovat päivittyneet uusimmassa Windows Server 2008 R2 -versiossa (taulukko 2). RDS-rooleja hallitaan seuraavilla hallintatyökaluilla (taulukko 3).

Taulukko 2. Terminal Services -roolien uudet ja vanhat nimet. (Anderson & Griffin 2010, 6.)

Roolien päivittyneet nimet	Roolien vanhat nimet
RD Session Host	Terminal Server
RD Virtualization Host	Uusi ominaisuus Windows Server 2008 R2:ssa
RD Connection Broker	TS Session Broker
RD Web Access	TS Web Access
RD Gateway	TS Gateway
RD Licensing	TS Licensing

Taulukko 3. RDS roolien hallintatyökalut (Anderson & Griffin 2010, 6.).

Roolien hallintatyökalujen päivittyneet nimet	Roolien hallintatyökalujen vanhat nimet
Remote Desktop Services Client Access License (RDSCAL)	Terminal Services Client Access License (TSCAL)
Remote Desktop Services Manager	Terminal Services Manager
Remote Desktop Services Configuration	Terminal Services Configuration

RD Session Host

Etäpöytäistunnon isäntä on yksi Remote Desktop Services -rooleista, jota pidetään hyvin keskeisenä osana Remote Desktop Services -arkkitehtuurissa. Tämän roolin tarkoituksena on toimittaa Windows-ohjelmia tai täyden etätyöpöytäyhteyden käyttäjälle. Kytkeytymällä RD Session Host -palvelimelle käyttäjä voi ajaa omalta työasemaltaan käsin palvelimelle asennettuja ohjelmia, tallentaa tiedostoja sekä käyttää verkon resursseja. (Microsoft Technet 2011.)

RD Virtualization Host

RD Virtualization Host -rooli on tullut uutena roolina Remote Desktop Services -kokonaisuuteen. Olennaisena osana RD Virtualization Host -rooliin kuuluu Hyper-V, joka on virtualisointityökalu, jolla voidaan luoda virtuaalikoneita. RD Virtualization Host -palvelimella voidaan konfiguroida kullekin käyttäjälle organisaatiossa henkilökohtainen virtuaalikone, johon asennetaan jokin käyttöjärjestelmistä; Vista, Windows 7 tai XP. Toinen tapa on antaa käyttäjälle virtuaalikone käyttöön poolista. (Microsoft Technet 2011.)

RD Web Access

RD Web Access tarjoaa etäkäyttäjille mahdollisuuden ajaa RD Session Host -palvelimelle asennettuja etäohjelmistoja selaimen kautta tai yksittäisinä ohjelmina työpöydiltä. Kyseinen rooli mahdollistaa myös käyttäjien Window 7 -työasemilta pääsyn etäohjelmiin ja virtuaalisiin työpöytiin käynnistä-valikon tai internetselaimen kautta. (Microsoft Technet 2011.)

RD Connection Broker

RD Connection Broker -roolin (etäpöytäistunnon välittäjä) tarve tulee silloin toteen, kun käytössä on yksi tai useampi RD Session Host -palvelin. Suuremmissa yrityksissä tarvitaan etäpalvelujen välittämisessä lukuisia RD Session Host -palvelimia, joilla varmistetaan etäpalvelujen saatavuus. Jotta etäpalveluita pyörittävien palvelimien kuormitus saadaan tasapainoon ja yhdelle palvelimelle kasautuva kuormitus ei heikentäisi sen toimintaa, käyttöön on otettava RD Connection Broker -rooli. (Microsoft Technet 2011.)

RD Gateway

RD Gateway -rooli toimii sisä- ja ulkoverkon välisenä yhdyskäytävänä. RD Gateway -roolipalvelussa määritellään ne käyttäjät, joilla on oikeus käyttää yrityksen sisäisen tai yksityisen verkon resursseja internetiin kytketyltä laitteelta, julkiselta tietokoneelta tai toimialueen asiakaspäätteeltä. RD Gateway käyttää etäyhteyksien turvaamiseen ja salaamiseen VPN:n sijaan RDP-over-HTTPS -protokollia. (Microsoft Technet 2011.)

RD Licensing

RD Licensing -rooli on järjestetty omana palveluna Remote Desktop Services -paketissa. Tämän roolipalvelun tarkoituksena on valvoa etäpöytäpalvelun käyttäjien lisensointia CAL (Client Access License). Kaikilla käyttäjillä tai laitteilla on oltava voimassaoleva lisenssi voidakseen toimia etäpöytäpalvelu-ympäristössä. (Microsoft Technet 2011.)

3.2 Remote Desktop Services -lisenssit

Etäpöytäpalvelun lisensointimalli sisältää neljä lisensointityyppiä: laitekohtaisen, käyttäjäkohtaisen, External Connector ja Services Provider License Agreement (SPLA) lisensointityypin. Etäpöytäpalvelun käyttö on mahdollista, jos RD session host -palvelimelle kytkeytyvällä käyttäjällä tai tietokoneella on voimassa ole-

va lisenssi. Jos lisenssi ei ole voimassa, etäpöytäpalvelua ei voida ottaa käyttöön. RD services -rooleja on mahdollista käyttää ilmaiseksi 120 päivän ajan, jonka jälkeen lisensointipalvelu on otettava käyttöön. (Anderson & Griffin 2010, 32.)

Käyttäjäkohtainen lisensointi

Kaikille käyttäjille annetaan henkilökohtainen lisenssi, jolloin RDS-roolipalveluita voi käyttää miltä tahansa koneelta (Andersson & Griffin 2010, 32).

Laitekohtainen lisensointi

Kaikki työasemat, jotka käyttävät RDS-roolipalveluita, tarvitsevat laitekohtaisen lisenssin. Tämä lisensointimalli on silloin käytännöllinen, kun samalla työasemalla on useita käyttäjiä. Jos käytössä on myös virtuaalityöasemia poolista tai henkilökohtainen virtuaalityöasema, tarvitaan myös laitekohtainen lisenssi. (Anderson & Griffin 2010, 645.)

RDS External Connector

RDS External Connector -lisensointityyppi antaa useille ulkoverkon käyttäjille (käyttäjille jotka eivät kuulu organisaatioon tai joille ei määritellä lisenssiä) pääsyn määrätylle palvelimelle. Jokainen ulkoverkon käyttäjälle hyväksytty palvelin tarvitsee lisenssin. Esimerkiksi jos halutaan lisensointi kahdelle RD session Host -palvelimelle, tarvitaan molemmille oma lisenssi. (Anderson & Griffin 2010, 645.)

Services Provider License Agreement (SPLA)

SPLA-lisensointityyppi on erityisesti tarkoitettu ICT-palveluyrityksille ja yksityisille palvelun myyjille, jotka järjestävät RDS-palveluita ja tarjoavat pääsyoikeuksia heidän RDS-palveluihinsa. Se on sovellusvuokrausta kuukausihinnoittelulla. (Anderson & Griffin 2010, 645.)

Kaikista neljästä eri lisensointivaihtoehdoista käytetyimpinä ovat käyttäjä- ja laitekohtaiset lisensoinnit. Isäntäpalvelimelle voi asentaa joko käyttäjä- tai laitekohtaisen lisenssin. Molempia ei voi käyttää samanaikaisesti. Molempien lisensointimallien käyttö on välttämätöntä, jos käyttöön otetaan VDI-palvelu. Käyttäjäkohtaisella lisensoinilla saadaan pääsy RD Session Host -palvelimille ja laitekohtaista lisensointia käytetään poolissa oleville ja henkilökohtaisille virtuaalityöasemille. (Anderson & Griffin 2010, 645.)

3.3 Laitevaatimukset

Mikäli käytetään rautapohjaista virtualisointia, on selvitettävä tukeeko kyseinen palvelin virtualisointiteknologiaa. Virtualisointituki löytyy ainakin Intel VT ja AMD-V -palvelimista ja lisäksi palvelimen täytyy olla 64-bittinen. Taulukossa 4 esitettään Microsoft Hyper-V Server 2008 R2:n laitevaatimukset.

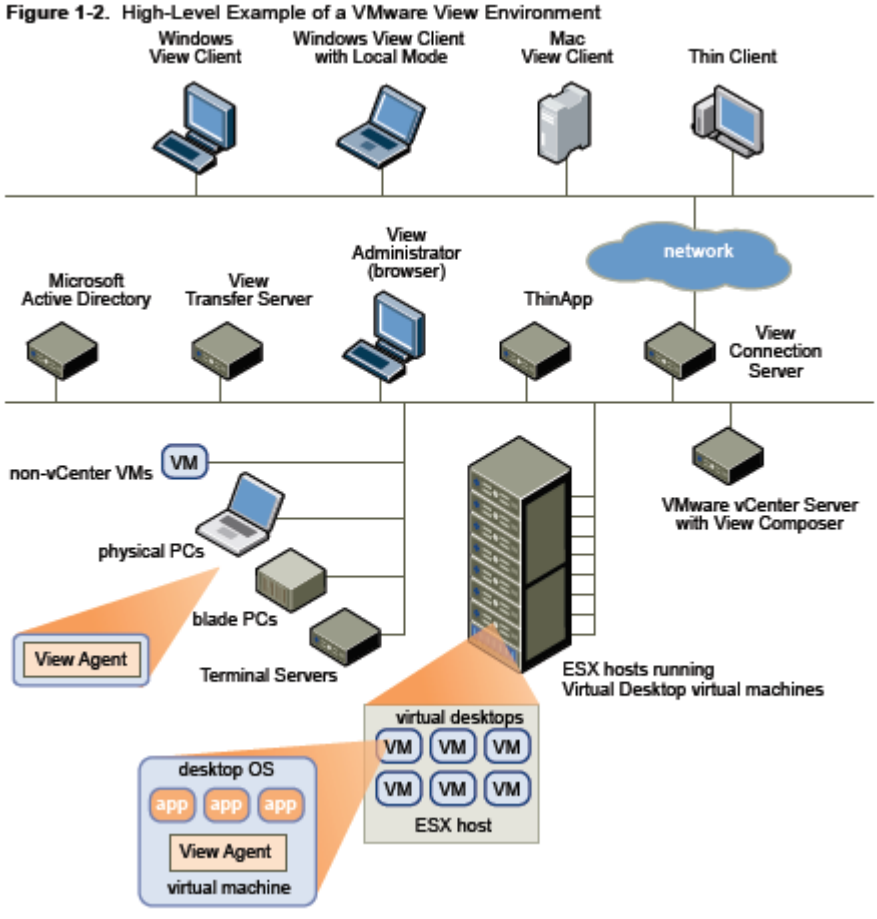
Taulukko 4. Microsoft Hyper-V Server 2008 R2 laitevaatimukset (Microsoft hyper-V 2011).

Toiminto	**Microsoft Hyper-V Server 2008 R2**
Prosessori	1.4 GHz (min), 2 GHz tai nopeampaa, Intel VT tai AMD-V teknologialla varustettu
RAM-muisti	1 GB (min), 2 GB tai enemmän (suositus), 1 TB (max)
Levyasema	DVD-ROM
Levykapasiteetti	8 GB (min), 20 GB tai enemmän
Näyttö	Super VGA (800 × 600) tai korkeampi resoluutio

4 VMWAREN VIRTUALISOINTIRATKAISU

4.1 VMware View

Tässä luvussa esitellään VMware View 4.5 kokoonpanoon kuuluvia komponentteja. Kuvassa 3 esitetään, mihin View-komponentit sijoittuvat verkkotopologiassa.



Kuva 3. VMware View -ympäristöön kuuluvat komponentit (VMware 2010b, 10).

View Client

View Client -sovellus asennetaan kaikkiin View-ympäristössä toimiviin Windows ja Mac PC-asiakaspäätteisiin. View Client -sovellusta käyttämällä saadaan asiakaspäätteestä yhteys View-työpöytiä jakavaan palvelimeen. Käyttäjäoikeuksien varmentaminen voidaan toteuttaa seuraavanlaisilla menetelmillä: Active Directory -käyttäjätietokannan tunnisteilla (käyttäjätunnus ja salasana), älykortin PIN-koodilla tai RSA Secure ID:llä (käyttäjätunnus, pin-koodi, vaihtuva varmisteavain). Clientin ja työpöytiä jakavan palvelimen välille voidaan asettaa etäkäyttöprotokollaksi PcoIP tai Micrsoftin RDP. HP RGS etäkäyttöprotokolla asetetaan View työpöydille, joiden isäntäpalvelimena toimii HP Blade. (VMware 2010b, 11.)

Asiakaspääte voidaan laittaa toimimaan myös Local Mode -tilassa, jota kutsutaan virallisesti nimellä Offline Desktop. Tällä ominaisuudella varustetun asiakaspäätteen ei tarvitse aina olla kytkettynä View-verkkoon, vaan jaettuja ohjelmistoja ja View-työpöytiä voidaan käyttää paikallisesti omalla päätteellä offline-tilassa. Kun asiakaspääte offline-tilan käytön jälkeen kytkeytyy uudelleen View-verkkoon, yhteydettömässä tilassa tehdyt muutokset päivitetään palvelua tarjoavalle palvelimelle. (VMware 2010b, 11.)

View Portal

View Portal järjestää asiakaspäätteelle mahdollisuuden käyttää View-palveluita verkkopohjaista selainta (Explorer, Firefox, Chrome) käyttäen. View Portaalin käyttöönottaminen tapahtuu avaamalla selain asiakaspäätteellä ja ottamalla yhteys View Connection Serverille. View Portaalin käyttöön saamiseksi asennetaan siihen tarvittavat client sovellukset. (VMware 2010b, 11.)

View Agent

View Agent -palvelu asennetaan kaikkiin niihin virtuaalikoneisiin, fyysisiin järjestelmiin ja Terminal Service -palvelimiin, jotka jaetaan käyttöön View-ympäristössä toimiville asiakaspäätteille. View Agent kommunikoi View Clientin

kanssa järjestämällä yhteyksien monitoroinnin, virtuaalitulostuksen ja pääsyn paikallisesti kytketyille USB-laitteille. (VMware 2010b, 12.)

Jos työpöytälähteenä on virtuaalikone, tulee ensimmäiseksi asentaa View Agent -palvelu virtuaalikoneeseen ja käytetään sitä mallivirtuaalikoneena, josta jatkossa voidaan luoda virtuaalikoneet nopeasti kopioimalla. Samasta mallivirtuaalikoneesta voidaan tehdä pooli, jolloin View-agentin asennus tapahtuu automaattisesti poolin luontivaiheessa. (VMware 2010b, 12.)

View Composer

View Composer on virtuaalikoneiden hallintaan tarkoitettu komponentti joka tulee asentaa samaan instanssiin vCenterin kanssa. View Composer ei ole välttämätön komponentti View-ympäristössä, mutta se tuo laajoihin View-ympäristöihin virtuaalikoneiden hallintaa helpottavia ominaisuuksia. View Composer -palvelun avulla voidaan luoda linked-clone pooli yhdestä levykuvasta. Tällä ominaisuudella saadaan vähennettyä tallennuskapasiteettia merkittävästi, jopa 50–90 %. (VMware 2010b, 12.)

View Transfer Server

Tämä ohjelmisto hallitsee ja välittää datan siirrot datakeskuksen ja View-työpöytien välillä. View Transfer -palvelua tarvitaan erityisesti silloin, kun View-työpöytiä halutaan käyttää Local Modina. View Transfer -palvelin on vaadittu tukemaan View Client -työpöytiä, jotka toimivat Local Modena. (VMware 2010b, 13.)

View Transfer -palvelu käyttää eri operaatioita lähettämällä dataa vCenterissä olevien View- työpöytien ja paikallisten työasemien välillä. Alla on Transfer Server -palveluun kuuluvia toimintoja (VMware 2010b, 13.):

- Kun käyttäjä kirjautuu työasemalle sisään tai siltä ulos, View Manager varmentaa ja hallitsee operaatiota.

- View Transfer Server päivittää paikallisella työasemalla tehdyt muutokset datakeskuksen vastaavalle työasemalle.
- Päivittämisaikavälit voidaan määritellä local-mode -käytännöissä ja View Administrator -käyttöliittymän kautta.
- View Transfer Server pitää huolen siitä, että paikalliset työasemat pysyvät ajan tasalla. Se jakaa järjestelmän tilatietoja datakeskuksilta paikallisille Client-työasemille.

View Connection Server

View Connection Server toimii asiakasyhteyksien välittäjänä. View Connection Server autentikoi käyttäjät Active Directoryn käyttäjäkannan avulla ja ohjaa pyynnöt sopivalle virtuaalikoneelle, fyysiselle PC:lle, blade-PC:lle tai Windows Terminal Services -serverille. Kyseinen komponentti voidaan asentaa neljään toimintatarkoitukseen, ensisijaiseksi palvelimeksi (standalone), ohjauspalvelimeksi (replica), Security-palvelimeksi tai Transfer-palvelimeksi. (VMware 2010a, 10-11.)

Ensimmäinen View Connection Server tulee asentaa standalone-asennuksena. Jos myöhemmin tarvitsee asentaa lisää Connection Server -palvelimia, ne asennetaan replica-asennuksena. Replica-asennusta käytetään skaalaamiseen ja kuorman tasaamiseen. Security-Server -palvelimen avulla voidaan toimittaa virtuaalinen työpöytä ulkoverkon käyttäjälle, jonka työasema on kytketty internetiin. (VMware 2010a, 10.)

View Connection Serverillä voidaan hallita myös seuraavanlaisia asioita (VMware 2010b, 10-11.):

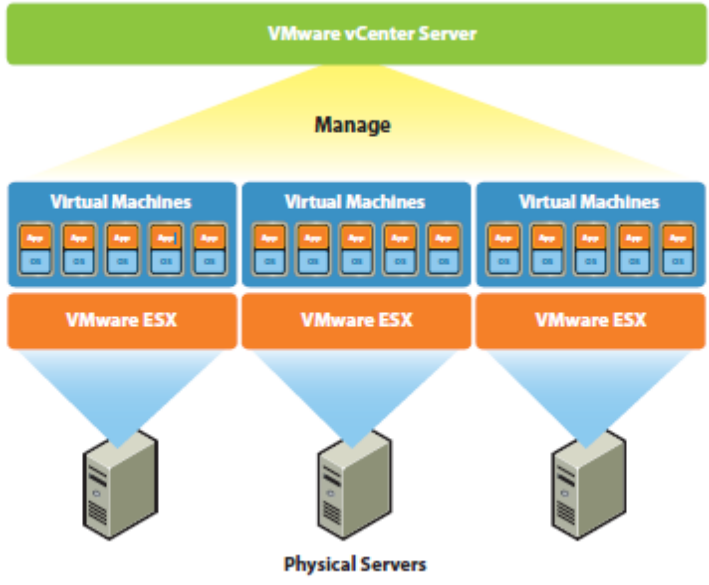
- käyttäjien autentikointi
- käyttäjien nimeäminen työpöydille ja pooleille
- VMwaren ThinApp:lla pakattujen sovellusten järjestäminen työpöydille ja pooleille
- paikallisten ja etätyöpöytäyhteyksien hallinta

- turvallisien yhteyksien järjestäminen.
- kertakirjautuminen (single sign-on)
- käytäntöjen määrittäminen.

View Connection Serveriä hallitaan web-pohjaisella View Administrator -hallintatyökalulla. View Administrator -hallintatyökalulla järjestetään ja hallitaan View-työpöytiä, kontrolloidaan käyttäjäntunnistusta sekä ratkotaan loppukäyttäjien ongelmia. View Administrator -hallintatyökalu asentuu View Connection Server -asennuksen yhteydessä, erillistä sovellusta View Connection Serverin hallintaan ei tarvitse asentaa paikalliselle koneelle. (VMware 2010b, 12.)

VMware vCenter

VMware vCenter on windows-pohjainen hallintajärjestelmä, joka tunnetaan virallisesti nimellä VMware Virtual Center. vCenter toimii keskitettynä hallintapisteenä useille ESX/ESXi isännille ja niiden virtuaalikoneille (kuva 4). vCenterin hallintapisteen kautta voidaan operoida virtuaalikoneiden konfigurointiin, provisiointiin, päivittämiseen ja hallintaan liittyviä toimintoja. (VMware vCenter 2010b, 12.)



Kuva 4. VMware vCenter Serverin toimintaperiaate (b2net, 2011).

vCenterin tehtäviä (Lowe 2009, 57-58):

- ESX/ESXi isäntien ja virtuaalikoneiden resurssien hallinta
- virtuaalikoneiden järjestäminen ja hallinta
- aikataulutetut toiminnot
- tilastotiedot ja kirjautumiset/rekisteröinnit
- hälytysten ja tapahtumien hallinta
- ESX/ESXi isäntien hallinta

Yksittäisessä vCenterin instassissa kyetään hallitsemaan 1000 isäntää (ESX/ESXi) ja 10 000 virtuaalikonetta. Linked-mode toiminnolla voidaan hallita 30 000 virtuaalikonetta, jotka jaetaan kymmeneen vCenter -instanssiin. vCenter palvelinta voidaan hallita työasemalta, johon on asennettu vSphere Client –sovellus. Samaa sovellusta käytetään yksittäisten ESX/ESXi-palvelimien hallintaan. (VMware 2011b.)

VMware ThinApp

VMware ThinApp kuuluu View-kokonaisuuteen sovellusvirtualisoinnin osalta. Sovelluksista paketoidaan itsenäisesti asennettavia, tietoturvallisesti kryptattuja exe-paketteja. ThinApp-teknologia mahdollistaa vanhempiin käyttöjärjestelmiin, Vistaan ja XP:hen, tarkoitettujen sovellusversioiden suorittamisen uudemmissa, esim. Windows 7 -käyttöjärjestelmissä. VMware ThinApp -teknologia säästää levyjärjestelmän tilaa ja kustannuksia, koska sovelluksien ei tarvitse olla työasemakuvissa (image) lainkaan. Sovelluksia voidaan toimittaa käyttäjille levyjaon, msi-paketoinnin tai USB-tikun kautta. (VMware ThinApp 2011c.)

4.2 Laitevaatimukset

Virtuaalikoneiden laitevaatimukset riippuvat käytössä olevasta vieraskäyttöjärjestelmästä ja samat vaatimukset pätevät myös fyysisissä tietokoneissa. Raskaampia ohjelmia käytettäessä virtuaalikoneisiin on varattava enemmän kapasiteettia. Taulukossa 5 on esillä Vmware ESXi:n laitevaatimukset. Taulukoissa 6 ja 7 esitetään käyttöjärjestelmäkohtaiset laitevaatimukset ja VMware View:n laitevaatimukset.

Taulukko 5. ESXi:n minimilaitevaatimukset (VMware 2011e).

Toiminto	**VMware ESXi 4.1**
Prosessori	AMD-64 (kaikki), Intel Xeon (64-bit): 3000/3200, 3100/3300, 5100/3300, 5200/5400, 7100/7300 ja 7200/7400 ja lisäksi Intel Nehalem.
Muistikapasiteetti	2 GB (min)
Verkkokortti	1 tai enemmän gigabit tai 10 GB
Levyohjain	SCSI: Adapter Ultra-160 tai Ultra-320. RAID: Dell Perc, HP Smart Array RAID tai IBM ServeRAID
Levyjärjestelmä	SATA, SCSI, Fibre Channel tai iSCSI

Taulukko 6. Virtuaalikoneisiin asennettavien Windows-käyttöjärjestelmien laitevaatimukset (VMware 2010b, 38-39).

Toiminto	Käyttöjärjestelmät		
	Windows XP 32-bit (viimeisin service pack)	Windows Vista 32-bit (viimeisin service pack)	Windows 7
Prosessori	1,3 GHz		1,6 GHz, Aero ominaisuuksia varten 2,2 GHz tai nopeampi
RAM	1GB, 512MB (min), 2GB (max)	1 GB	1 GB
Järjestelmän levykapasiteetti	16GB, 8GB (min), 40GB (max)	20 GB	20 GB
Käyttäjän levykapasiteetti	5GB	5 GB	5 GB

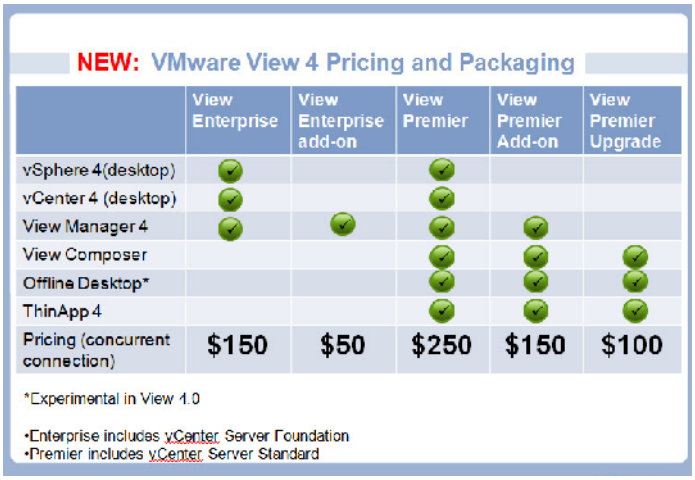
Taulukko 7. VMware View:n komponenttien laitevaatimukset (VMware 2011e, 15 ja VMware 2011f).

Toiminnot	VMware View -komponentit	
	View Connection Server	**vCenter**
Käyttöjärjestelmä	Windows Server 2008 64-bit	Windows Server 2008 64-bit
Prosessori	Pentium IV 2.0 GHz tai korkeampi (tuplaprosessori)	2 GHz (Intel tai AMD)
RAM	4 GB tai enemmän. 10 GB 50 View-työpöydälle.	3 GB (min)
Levykapasiteetti	40 GB	3 GB (min)
Verkkokortti	Yksi tai enemmän 10/100Mbps (suositus 1Gbps)	1 GB (suositus)

4.3 Lisenssit

VMware View -lisenssit myydään nippuperiaatteella ja ne on järjestetty kahteen eri kategoriaan, saatavilla on Enterprise ja Premier -versiot (taulukko 8). Halutessaan olemassa olevia kokoonpanoja voi täydentää hankkimalla lisäominaisuuksia Add-on-merkinnöillä. (VMware 2011d.)

Taulukko 8. VMware View -komponenttien hinnoittelu (VMware 2011d).



NEW: VMware View 4 Pricing and Packaging

	View Enterprise	View Enterprise add-on	View Premier	View Premier Add-on	View Premier Upgrade
vSphere 4(desktop)	✓		✓		
vCenter 4 (desktop)	✓		✓		
View Manager 4	✓	✓	✓	✓	
View Composer			✓	✓	✓
Offline Desktop*			✓	✓	✓
ThinApp 4			✓	✓	✓
Pricing (concurrent connection)	$150	$50	$250	$150	$100

*Experimental in View 4.0

•Enterprise includes vCenter Server Foundation
•Premier includes vCenter Server Standard

View-tuotteita voi hankkia 10 ja 100 kappaleen erissä. 10 kappaleen nippu sisältää vCenter Foundationin, joka on rajoitettu kolmeen isäntään. 100 kappaleen nippu sisältää vCenter Server Stardardin, jossa isäntien määrää ei ole rajoitettu. Molemmat niput sisältävät vSphere 4 for Desktops -komponentin. (VMware 2011d.)

5 SUUNNITTELU

Työpöytä- ja sovellusvirtualisointiympäristö rakennetaan Pohjois-Karjalan AMK:n Wärtsilä toimipisteen tietoliikennelaboratoriossa opetuskäyttöön 10-20 henkilölle. Etäkäyttöympäristö tehdään testitarkoituksessa, varsinainen etäpöytäsysteemi suunnitellaan, rakennetaan ja myöhemmin sitten jalostetaan täsmällisemmin vaadittujen kriteereiden mukaiseksi. Tässä luvussa esitetään opinnäytetyössä toteutettavien Microsoftin Remote Desktop Services ja VMwaren View testiympäristöt sekä kuvataan niihin tehtävät asennusvaiheet.

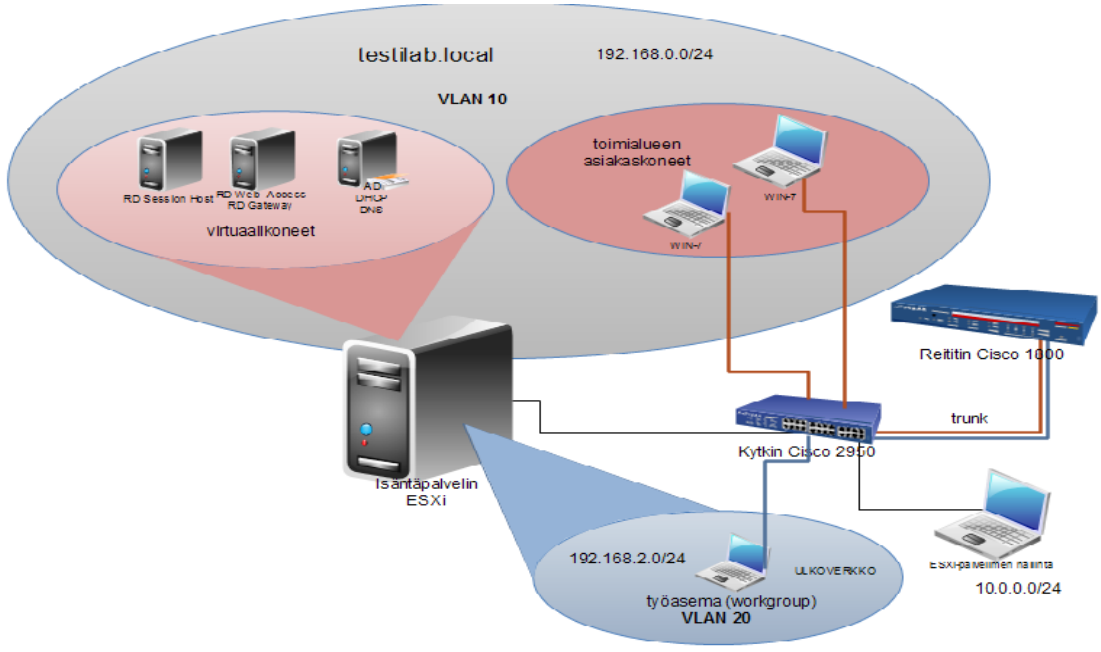
Etäpalveluympäristöä suunnitellessa nyrkkisääntönä on hyvä pitää sitä, että kahdeksan virtuaalikonetta voidaan asentaa yhtä prosessoria kohden, jos muut (muisti, levytila) vaatimukset täyttyvät. Prosessorimäärien lisäksi pitää huomioida, että muistia ja tallennuskapasiteettia on varattu riittävästi. (Ruest & Ruest 2009, 126.)

Koulu antoi etäpöytäpalvelun rakentamiseen käyttöön HP-palvelimen. HP-palvelimen tekniset tiedot on esitetty alla taulukossa 9.

Taulukko 9. HP-palvelimen tekniset tiedot.

HP ProLiant ML 350 G5
Prosessori Intel Xeon E5420 4 x 2,5 GHz
NICs 1
Levykapasiteetti 131,75 GB (RAID 1)
Muisti 6 GB

Kuvassa 5 on esitetty Microsoft Remote Desktop Services -testiympäristön verkkotopologia.



Kuva 5. Microsoft Remote Desktop Services -testiympäristön verkkotopologia.

Testiympäristön verkkoinfrastruktuuriin kuuluu HP-palvelimen lisäksi Ciscon 2900 sarjan kytkin, 1800 sarjan reititin ja Windows 7 -työasemia.

Projektin ensimmäisenä toimenpiteenä on asentaa virtualisointialusta, jonka päälle koko systeemi rakennetaan. VMware Esxi 4.1 virtualisointijärjestelmä asennetaan HP-palvelimelle, jolla luodaan virtuaalikoneet. Virtuaalijärjestelmäksi voitaisiin asentaa myös Microsoftin oma Hyper-V. Luotuihin virtuaalikoneisiin asennetaan Windows Server 2008 Standard R2 käyttöjärjestelmä. VMware ESXi virtualisointityökalulla luodaan mallipalvelin, johon on valmiiksi asennettu käyttöjärjestelmä. Jatkossa uusia palvelimia voidaan luoda kopioimalla mallipalvelimesta vmx-tiedosto uuteen virtuaalikoneeseen.

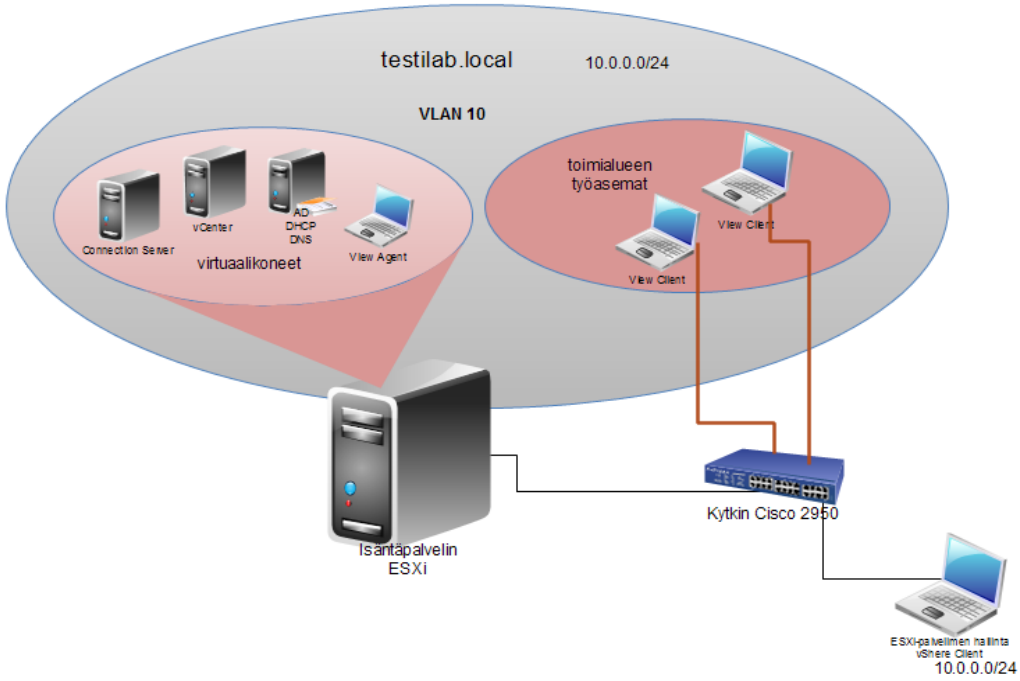
Työ etenee Remote Desktop services roolien ja AD-palvelimien asennuksella. Windows 2008 server R2 käyttöjärjestelmä sisältää RDS-palvelun. Roolien asennukset toteutetaan Server Managerissa**.** AD-palvelimella perustetaan toimialue ja lisätään etäpöytäpalvelua käyttävät käyttäjät. Etäpöytäpalvelun käyttäjille kannattaa luoda oma ryhmä hallinnan helpottamiseksi. Palvelimille asennetaan F-secure tietoturvaohjelmisto ja update-päivitykset. Etäpöytäpalveluja on tarkoitus testata myös ulkoverkon kautta. Sitä varten tehdään ESXi virtualisointityökalulla ulkoverkolle aliverkko VLAN 20 ja sisäverkolle VLAN 10. Tämän jälkeen konfiguroidaan kytkimillä portit aliverkoille. Testiympäristöön otetaan käyttöön myös reititin, jonka tarkoituksena on toimia yhdyskäytävänä VLAN:ien välillä. Reitittimen ja kytkimen välille konfiguroidaan trunk-yhteys. Konfiguraatiot löytyvät liitteeistä 4 ja 5.

RDS sisältää kuusi erilaista roolia. Suunnitteluvaiheessa on hyvä tarkoin selvittää mitä rooleja tarvitsee. Jos kaikki roolit otetaan käyttöön, roolien toimintakuva vaihtuu. Tässä projektissa käytetään seuraavia rooleja: RD Session Host, RD Web Access ja RD Gateway. RD Session Host asennetaan omalle virtuaalikoneelle ja RD Web Access ja RD Gateway asennetaan keskenään samalle virtuaalikoneelle. Jos kyseessä on tuotantoympäristö, jälkimmäiset roolit kannattaa asentaa DMZ-ympäristöön tietoturva syistä (Anderson & Griffin 2010, 576-577).

RD connection broker ja RD virtualization host -roolit jätetään tässä projektissa asentamatta. RD connection broker -roolia tarvittaisiin, jos etäpöytiä ja ohjelmistoja julkaisevia palvelimia (RD Session Host) olisi useampi kuin yksi. RD Virtualization Host -palvelu oli tarkoitus ottaa testaukseen tässä projektissa, mutta palvelun käyttöönotto estyi, koska virtualisointialustaksi asennettiin VMwaren ESXi. RD virtualization -palvelu suostuu nimenomaan yhteistyöhön vain oman Hyper-V:n kanssa.

Etäpöytäpalveluiden roolien asennusten jälkeen kyseiset palvelimet liitetään testilab.local toimialueeseen ja tehdään peruskonfiguraatiot (liitteessä 1) sekä suoritetaan etäpöytäjärjestelmän testaukset. Niistä kerrotaan myöhemmin omassa luvussaan.

Kuvassa 6 on esitetty VMwaren View -testiympäristön verkkotopologia. VMware View:n kokoonpanossa käytetään samoja laitteita, mitä käytettiin Microsoftin testiympäristössä, mutta rakennettu testiympäristö on toiminnallisesti ja kokoonpanoltaan suppeampi.



Kuva 6. VMware View -testiympäristön verkkotopologia.

VMware View -ratkaisulla testataan VDI-ominaisuuden toimivuutta. Testiympäristössä käytetään samaa AD-palvelinta, jota käytettiin Microsoft RDS-ympäristössä. AD-palvelimelle muutetaan vain IP-osoite käyttämään 10.0.0.0/24 verkkoa.

VMware View -testiympäristöön luodaan AD-palvelimen lisäksi kaksi virtuaalipalvelinta ja yksi virtuaalityöasema. Virtuaalikoneisiin asennetaan Windows Server 2008 R2 käyttöjärjestelmä ja virtuaalityöasemaan WIN-7 käyttöjärjestelmä. Virtuaalikoneisiin konfiguroidaan IP-osoitteet 10.0.0.0/24 verkosta ja ne liitetään testilab.local -toimialueeseen.

Testiympäristön rakentamista jatketaan View-komponenttien asennuksella. Connection server -komponentti asennetaan toiseen virtuaalipalvelimeen ja toiseen asennetaan vCenter -komponentti. Molemmat asennukset suoritetaan tavallisesti Windows Server 2008 R2 -käyttöjärjestelmässä. Asennusohjeet löytyvät liitteestä 2. Asennusten jälkeen tehdään konfiguroinnit (liite 2) ja suoritetaan testaukset (kuvataan luvussa 6).

6 TESTIYMPÄRISTÖJEN TESTAUS

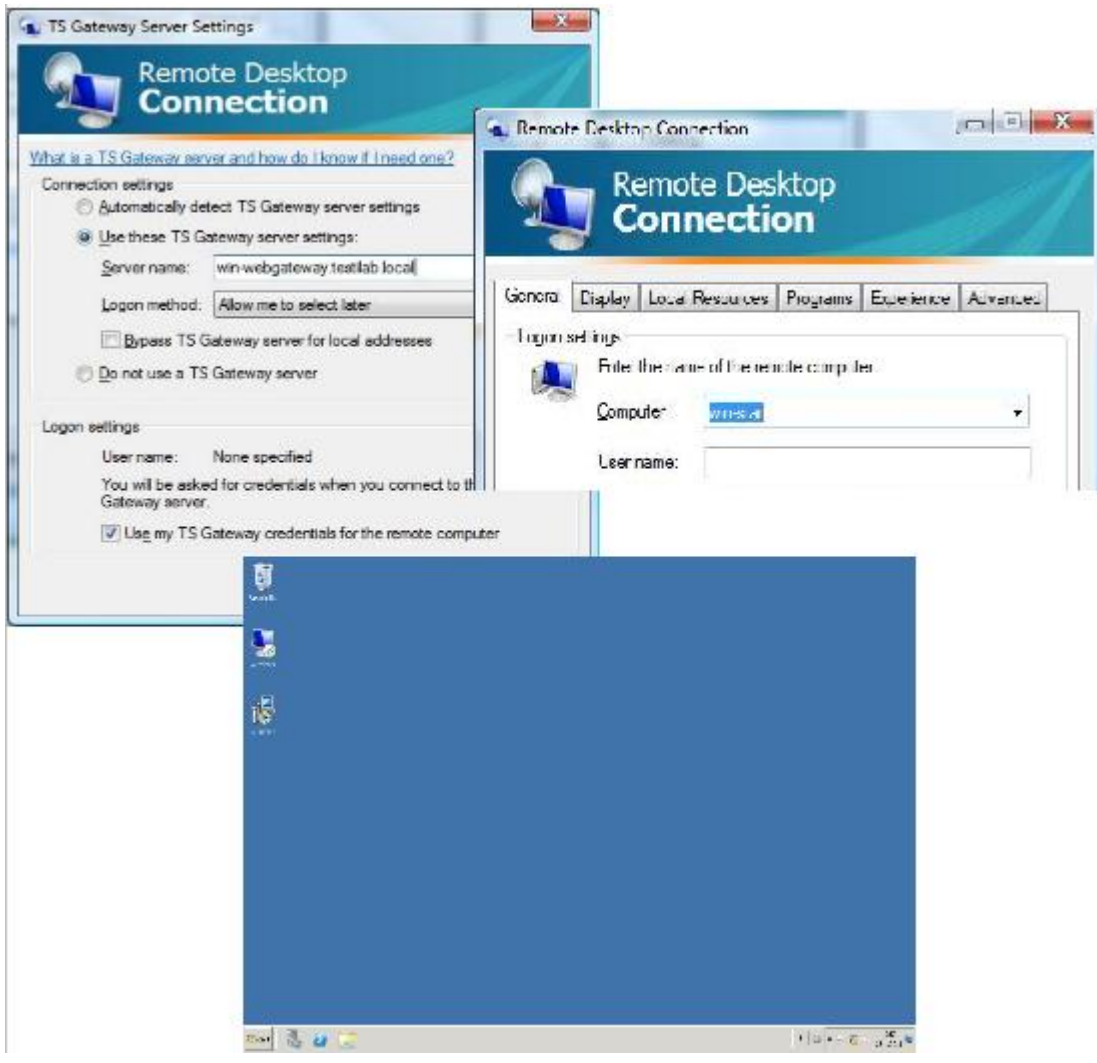
Opinnäytetyössä tehtiin VMwaren ja Microsoftin -virtualisointiratkaisuilla testiympäristöt. Microsoftin osalta testiympäristön kokoonpano oli laajempi kuin VMwaren. Kummatkin testiympäristöt tehtiin samalle HP-palvelimelle ESXi-virtualisointijärjestelmää käyttäen. Laitteistojen kokoonpanot ovat nähtävissä suunnitteluosiossa.

6.1 Microsoft RDS testaus

Microsoftilla rakennettua Remote Desktop Services -testiympäristöä testattiin testilab-toimialueen työasemilla ja ulkoverkon työasemalla (workgroup). Työasemilta otettiin yhteys etäpöytäjärjestelmään käyttämällä RDC-etäpöytäohjelmistoa tai internetselainta. Näillä client-sovelluksilla saatiin käyttöön jaettu etätyöpöytä tai yksittäisiä ohjelmia.

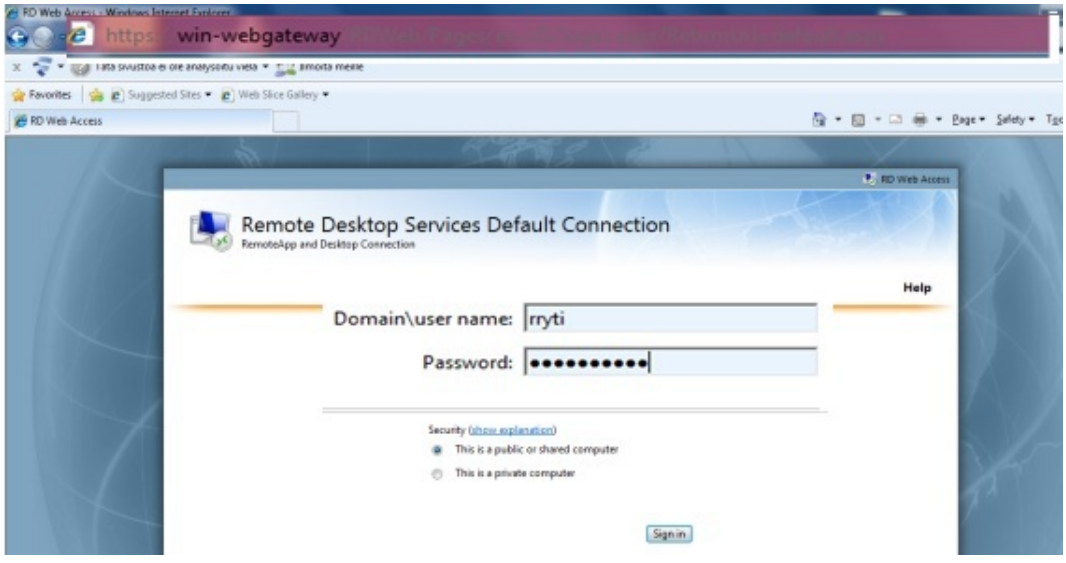
Täyden etätyöpöydän voi ottaa käyttöön RDC-etäpöytäsovellusta käyttämällä. Toimialueen käyttäjätunnuksella kirjauduttiin normaalisti Windows 7 -työasemalle. Työasemalla etäohjelmistojen tai virtuaalisten työpöytien käyttöönotto voidaan tehdä kahdella eri tavalla: käyttämällä Windowsin omaa etäpöytäohjelmistoa (Remote Desktop Connection) tai internetselainta. Etäpöytäohjelmiston virtuaalinen työpöytä varataan käyttöön käynnistämällä etäpöytäohjelmisto käynnistä-valikosta, josta valitaan ensin ”Accessories” ja sen jälkeen ”Remote Desktop Services”.

Koska testiympäristössä asiakaspäätteeltä terminaalipalvelimelle lähtevät pyynnöt menevät RD Gateway -palvelimen kautta, RDC:llä tarvitsee tehdä muutamia asetuksia. RDC-ikkunassa painetaan “Options” nappia ja valitaan välilehdeltä “Advanced” sekä klikataan “Settings”. Tehdään RD Gateway -asetukset lisäämällä palvelimen nimi toimialuenimineen, valitaan kirjautumisessa käytettävä varmistusta ja rasti pois kohdasta “Bypass TS Gateway server for local address” (kuva 7). Palvelimen nimeksi win-webgateway.testilab.local ja “General” välilehdeltä käynnistetään etäpöytäyhteys kirjoittamalla terminaalipalvelimen nimi “WIN-STAR” tai sen IP-osoite. Ennen kuin virtuaalinen työpöytä avautuu, järjestelmä kysyy etäpöytäpalvelun asiakkaan tunnuksia. Lisätään tunnukset, minkä jälkeen virtuaalinen työpöytä avautuu profiiliasetuksineen.

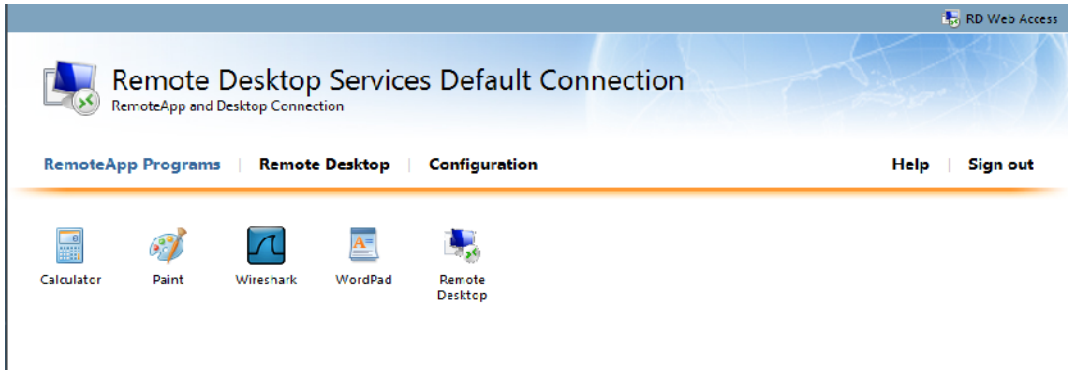


Kuva 7. RDC-etäpöytäsovelluksella virtuaalisen työpöydän noutaminen.

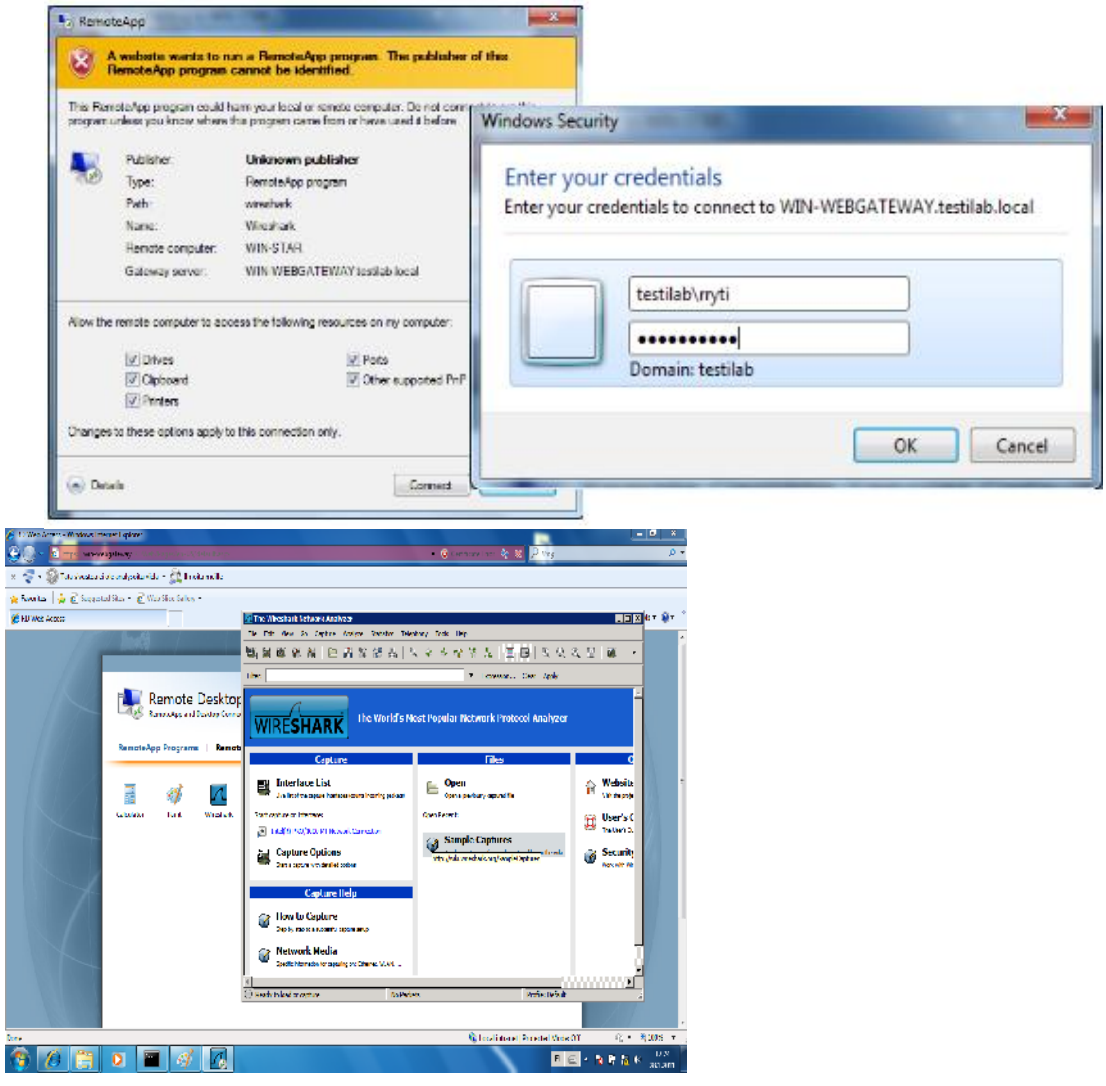
Toinen tapa käyttää etäpöytäpalvelun tarjoamia palveluita on internetselaimen kautta. Käynnistetään internetselain (Explorer, Firefox, Chrome) ja kirjoitetaan selaimen osoitekenttään RD Web Access -palvelimen osoite: https://win-webgateway/rdwebn (kuva 8). Tämän jälkeen ruudulle avautuu RD Web Access kirjautumisikkuna. Kirjaudutaan sisään seuraavilla tunnuksilla: käyttäjätunnus “rryti” ja salasana. Lopulta etäohjelmalistalle tulee esiin ne ohjelmat, joita kirjautuneella käyttäjällä on oikeus käyttää. Etäohjelma käynnistetään klikkaamalla kuvaketta ”Wireshark” (kuva 9). Syötetään käyttäjätunnukset ohjelmaan kirjauduttaessa (kuva 10).



Kuva 8. RD Web Access -kirjautumisikkuna.



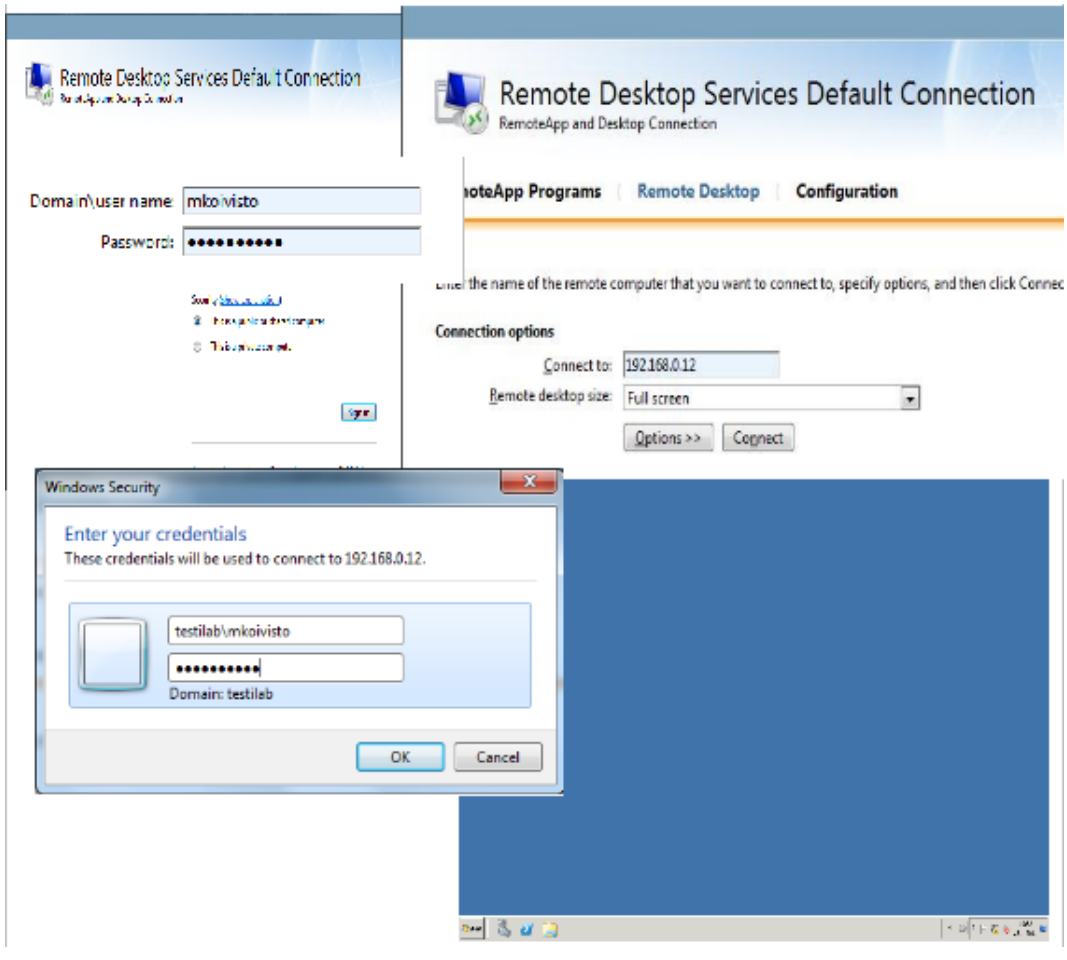
Kuva 9. Etäohjelmat.



Kuva 10. Kirjautuminen Wireshark-etäohjelmaan.

Etäpöytäpalvelun toimivuutta testattiin myös ulkoverkon työasemalta, joka ei kuulunut testilab-toimialueeseen. Ulkoverkon Windows 7 -työasemalta otettiin yhteys internetselaimen kautta etäpöytäpalvelujärjestelmään osoitteella: https://192.168.0.14/rdweb. Haku tehdään IP-osoitetta käyttäen, koska DNS-palvelinta ei ole käytössä. Sen jälkeen kirjaudutaan normaaliin tapaan etäpöytä-järjestelmään toimialueen käyttäjätunnuksilla ”mkoivisto” ja ”salasana” (kuva 11). Seuraavaksi ”Remote Desktop” -välilehdellä lisätään RD Session Host -palvelimen IP-osoite ja painetaan ”Connect”. Sen jälkeen järjestelmä kysyy

käyttäjätunnusta ja salasanaa. Kirjaudutaan toimialueen käyttäjätunnuksilla seuraavasti: testilab\mkoivisto ja salasana. Kirjautumisvaiheiden jälkeen ruudulle avautuu jaettu etätyöpöytä profiiliasetuksineen.



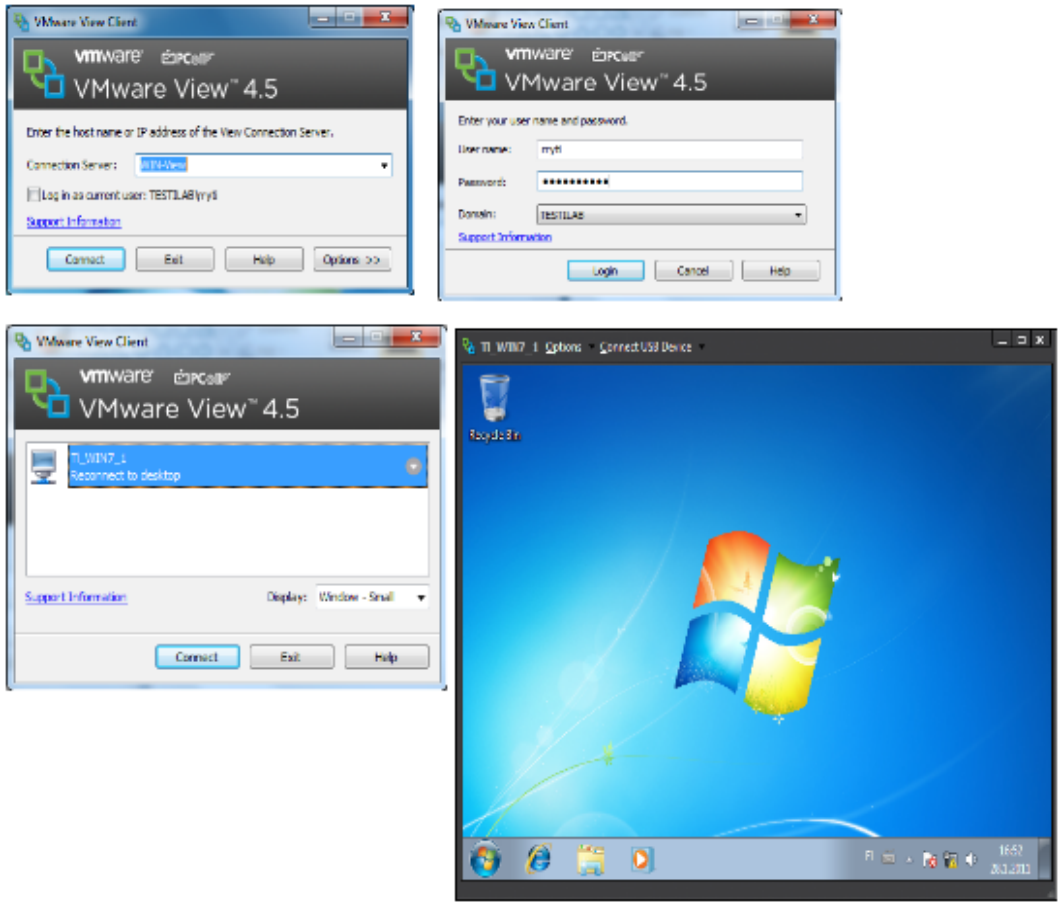
Kuva 11. Etäpöytäjärjestelmän testaaminen ulkoverkon työasemalta internetselaimen kautta.

Testiympäristössä testattiin vielä sovellusvirtualisoinnin tuomia ominaisuuksia. Luotiin .rdp ja .msi -tiedostot. Rdp-tiedoston luonnilla tarjotaan käyttäjille mahdollisuus käynnistää yksittäinen ohjelma omalta työpöydältä. Msi-tiedoston luonnilla saadaan toimitettua etäpöytäjärjestelmän käyttäjille halutun sovelluksen asennustiedosto, jonka he voivat asentaa omalla työasemallaan käynnistettäväksi työpöydältä tai käynnistä-valikosta (kuva 12).

Kuva 12. msi-tiedosto käynnistä-valikossa ja työpöydällä sekä .rdp-tiedosto työpöydällä

6.2 VMware View testaus

VMware View -virtualisointiratkaisulla tehtiin VDI-ympäristö. Toimialueen työasemalta otettiin yhteys View-Clientillä virtuaalisia työpöytiä jakavaan View Connection -palvelimeen ja pyydettiin toimialueen käyttäjälle nimetty Windows 7:llä varustettu virtuaalityöasema käyttöön. Kuvassa 13 kuvataan niitä vaiheita, jotka liittyvät työpöydän noutamiseen.



Kuva 13. View-työpöydän noutaminen.

7 POHDINTA

Tässä opinnäytetyössä tehtiin testiympäristöt VMwaren ja Microsoftin tarjoamilla virtualisointiratkaisuilla. Näiden virtualisointiratkaisuiden toteutetut kokoonpanot eivät olleet toiminnaltaan keskenään verrattavia, koska Microsoftin Remote Desktop Services -kokoonpanon osalta ei voitu rakentaa VDI-ympäristöä. VDI-ratkaisun pystyttämiseen olisi tarvittu RDS:n RD Virtualization Host -rooli ja se olisi vaatinut virtualisointialustaksi Microsoftin oman hyper-V:n. Sen sijaan palvelimelle oli asennettu VMware ESXi 4.1. Työtä jatkettiin niillä komponenteilla, joita oli siihen mennessä asennettu ja päädyttiin ratkaisuun tekemällä terminaalipalvelu Microsoft RDS -rooleilla. Koska VDI-ympäristöä ei kyetty pystyttämään Microsoftin tarjoamalla tuotteella, se tehtiin VMwaren ratkaisulla. VMware View:n VDI-ympäristön pystyttäminen onnistui ilman suurempia ongelmia.

Työstä ei selvitty aivan ongelmitta. Ongelmia ilmeni testattaessa Remote Desktop Services -virtualisointiratkaisun tarjoamia palveluita toimialueen ja ulkoverkon työasemilta. Ensimmäinen ongelma oli toimialueen työasemalla, kun etäohjelmat eivät käynnistyneet internetselaimen kautta. Etäohjelmien kuvakkeet tulivat esille käyttöliittymässä, mutta ne eivät suostuneet avautumaan. Ongelmia aiheutti se, että ulkoverkon työasemalta ei pystytty avaamaan etäohjelmia selaimen kautta eikä pystytty noutamaan etätyöpöytää terminaalipalvelimelta.

Ongelmia selvitettiin tutkimalla RD Gateway -palvelimen lokeja, koska kaikki terminaalipalvelimelle (RD Session Host) menevät pyynnöt menivät RD Gateway -roolin kautta. Lokeista sai selville, mihin palvelupyynnöt pysähtyivät. Lokeissa esiintyviä vikakoodeja lukemalla sai selville mihin ongelmat liittyivät ja tarkemmat tiedot sai syöttämällä vikakoodin numeron Technet-websivustolla. Käymällä läpi Technet-websivustolta saadun tarkistuslistan, selvisi todellinen ongelma; AD-palvelimen konfiguraatioissa oli puutteita.

Toimialueen tietokoneet piti liittää erikseen ryhmiin, joilla oli etäpöytäpalveluiden käyttöoikeus. Tietokoneet löytyivät käynnistä-valikon kautta valitsemalla Administrator Tools, Active Directory Users and Computers ja Computers. Tietokoneet lisättiin ryhmiin klikkaamalla oikeanpuoleista nappia ja valitsemalla ”Add groups”. Tietokoneet lisättiin ryhmiin, joihin etäpöytäpalvelua käyttävät käyttäjät oli lisätty. Näiden toimenpiteiden jälkeen etäpöytäpalveluiden testaaminen onnistui ongelmitta. Etäohjelmien avaaminen toimialueen työasemilta käsin toimi hienosti ja samoin etäpöytäpalveluiden testaaminen ulkoverkosta saatiin toimimaan.

Opinnäytetyössä ei ehditty pystyttää varsinaista opetusympäristöä, koska itse järjestelmän pystyttämiseen meni paljon aikaa. Opetusympäristö oli tarkoitus tarjota palveluna 10-20 henkilölle. Palvelun järjestäminen terminaalipalvelulla olisi varmasti ollut teknisesti mahdollista, koska se olisi vienyt vähemmän kapasiteettia. VMwaren VDI-ratkaisun tarjoaminen mainitun kokoiselle ryhmälle olisi kuitenkin tuonut teknisisiä rajoituksia rajallisen levytilan ja muistin vuoksi.

Testiympäristöjen asennusten ja käyttöönottojen helppoutta ei voi keskenään verrata niiden poikkeavuuksien takia, mutta silti VMwaren komponenttien käyttöönotto lyhyen kokemuksen perusteella vaikuttaa Microsoftin virtualisointiratkaisuihin nähden helpommalta. VMwaren pitempiaikainen kokemus virtualisointituotteiden valmistajana näkyy selkeästi heidän tuotteissaan.

Tämän opinnäytetyöprojektin tuomien kokemusten perusteella uskon, että työpöytä- ja sovellusvirtualisointi jatkavat kasvuaan virtualisoinnin markkinoilla. Kyseiset virtualisoinnin muodot ovat käytettävyyden, hallinnan ja kustannusten kannalta niin hyödyllisiä teknologiamuotoja, että monet tahot pitävät niitä potentiaalisina vaihtoehtoina IT-infrastruktuurin muutoksissa. Työpöytä- ja sovellusvirtualisoinnin rajoitteena ei ainakaan ole se, että etäpöytäjärjestelmän asiakaspäätteen tarvitsisi olla aina kiinteästi kytkettynä etäpöytäjärjestelmään. VMwarella etäohjelmia ja virtuaalisia työpöytiä voidaan käyttää yhteydettömässä tilassa (Offline desktop). Sovellusvirtualisointi tuo helpotusta siten, että vaikeasti asennettavat ohjelmat tarvitsee asentaa ainoastaan yhteen paikkaan (palveli-

melle) ja laitevaatimuksien tarvitsee täyttyä vain sillä palvelimella, johon ohjelmat asennetaan. Ohjelmien päivittäminen tapahtuu kätevästi ja ohjelmien välittäminen monille käyttäjille voidaan tehdä hyvinkin nopeasti muutamalla hiiren klikkauksella.

Opinnäytetyö oli erittäin opettavainen ja mielenkiintoinen projekti. Opinnäytetyössäni pääsin käsittelemään ja oppimaan juuri sellaisia asioita mitä olin toivonut. Opettavaisina asioina olivat työpöytä- ja sovellusvirtualisoinnin lisäksi palvelinhallinta, kytkimen ja reittimen konfigurointi sekä verkon konfigurointeihin liittyvät toimet. Kertyneitä kokemuksiani voin varmasti hyödyntää tulevaisuudessa, jos samankaltaisia työtehtäviä ilmenee.

Tästä päättötyöstä voidaan kehittää loistavia jatkokehitystöitä. Microsoftin osalta tietenkin VDI-ratkaisun pystyttäminen olisi testaamisen arvoinen työ. VMwaren puolelta löytyy paljon virtualisointimahdollisuuksia. ThinApp:a ja erityyppisten poolien sekä offline desktopin ominaisuuksia voisi olla hyvä testata. Citrix jäi kokonaan tämän opinnäytetyön ulkopuolelle. Citrixiltä löytyy vastaavanlaisia virtualisointiratkaisuja kuin Microsoftilta ja VMwarelta.

LÄHTEET

Anderson, C. & Griffin, K. 2010. Remote Desktop Services Resource Kit. Washington: Microsoft Press.

Atea 2011a. SAMK virtualisoi edelläkävijänä opiskelijoiden työpöydät. Atea: http://www.atea.fi/default.asp?P=6687 Viitattu 24.2.2011.

Atea 2011b. Pohjois-Karjalan ammattikorkeakoulu virtualisoi: Atea ja Citrix puhdistivat opiskelijoiden työpöydät. Atea: http://www.atea.fi/default.asp?P=6699 Viitattu 24.2.2011.

Bolton, D. 2011. Definition of Virtualization. About: http://cplus.about.com/od/glossar1/g/virtualization.htm Viitattu 24.2.2011.

b2net 2011. VMware vCenter Server. http://www.b2net.co.uk/VMware/VMware_vCenter_server.htm Viitattu 24.2.2011.

Desai, A. 2007. Virtual Platform Management. San Francisco: Realtime Publishers.

Lowe, S. 2009. Mastering VMware vSphere 4. Kanada: Wiley Publishing,Inc.

Microsoft Technet 2011. Overview of Remote Desktop Session Host. Microsoft: http://technet.microsoft.com/en-us/library/cc742806.aspx Viitattu 24.2.2011.

Microsoft Technet 2011. Overview of RD Virtualization. Mircosoft: http://technet.microsoft.com/en-us/library/dd759170.aspx 24.2.2011 Viitattu 24.2.2011.

Microsoft Technet 2011. Overview of Remote Desktop Web Access. Microsoft: http://technet.microsoft.com/en-us/library/cc772452.aspx Viitattu 24.2.2011.

Microsoft Technet 2011. Overview of Remote Desktop Connection Broker. Microsoft: http://technet.microsoft.com/en-us/library/cc772245.aspx Viitattu 24.2.2011.

Microsoft Technet 2011. Remote Desktop Gateway. Microsoft: http://technet.microsoft.com/en-us/library/dd560672%28WS.10%29.aspx Viitattu 24.2.2011.

Microsoft Technet 2011. Overview of Remote Desktop Licensing. Microsoft: http://technet.microsoft.com/en-us/library/cc725933.aspx Viitattu 24.2.2011.

Microsoft hyper-V 2011. System Requirements. Microsoft: http://www.microsoft.com/hyper-v-server/en/us/system-requirements.aspx Viitattu 24.2.2011.

Mäntylä, J-M. 2008. Virtualisointi mullistaa tietotekniikan. Tietoviikko:

http://www.tietoviikko.fi/cio/article192316.ece Viitattu 23.2.2011.
Ruest, D. & Ruest, N. 2009. Virtualization A Beginner's Guide. New York: Mc Graw Hill.

Ruest, D. & Ruest N. 2008. Use application virtualization before moving to VDI. SearchVirtualDesktop: http://searchvirtualdesktop.techtarget.com/tip/Use-application-virtualization-before-moving-to-VDI Viitattu 24.2.2011.

Rule, D. & Dittner, R. 2007. The Best Damn Server Virtualization Book Period. Burlington: Syngress Publishing, Inc

VMware 2010a. A Guide to Large-scale Enterprise VMware View 3 and VMware View 4 Deployments. VMware: http://www.VMware.com/files/pdf/resources/VMware-view-reference-architecture.pdf Viitattu 23.2.2011.

VMware 2010b. VMware View Architecture Planning Guide. VMware: http://www.VMware.com/pdf/view45_architecture_planning.pdf Viitattu 24.2.2011.

VMware 2011a. History of Virtualization. http://www.VMware.com/virtualization/history.html Viitattu 24.2.2011.

VMware 2011b. VMware vCenter server features. VMware: http://www.VMware.com/products/vCenter-server/features.html Viitattu 24.2.2011.

VMware 2011c. VMware THinapp features. VMware: http://www.VMware.com/products/thinapp/features.html Viitattu 24.2.2011.

VMware 2011d. VMware View 4 FAQ: Picing, Licensing and Support. VMware:https://images01.insight.com/media/pdf/View4LicensingFAQ.pdf Viitattu 24.2.2011.

VMware 2011e. ESXi Installable and vCenter Server Setup Guide. VMware: http://www.VMware.com/pdf/vsphere4/r41/vsp_41_esxi_i_vc_setup_guide.pdf Viitattu 24.2.2011

VMware 2011f. VMware View Installation Guide. VMware: http://www.VMware.com/pdf/view45_installation_guide.pdf Viitattu 24.2.2011.

Wikipedia 2011. Virtual Machine. Wikipedia: http://en.wikipedia.org/wiki/Virtual_machine Viitattu 24.2.2011.

MICROSOFT RDS -ROOLIEN ASENNUS JA KONFIGURAATIOT

1. DOMAIN CONTROLLER ASENNUS; DNS, DHCP, toimialue
2. RDS roolien asennus ja konfigurointi
3. Testiympäristön testaus

Remote Desktop Services –roolien asennuksessa käytettiin seuraavia lähdemateriaaleja, jotka on tulostettu 24.11.2010:

Installing Remote Desktop Session Host Step-by-Step Guide http://go.microsoft.com/fwlink/?LinkId=147293

Deploying Remote Desktop Gateway Step-by-Step Guide http://go.microsoft.com/fwlink/?LinkId=142251

Anderson, C. & Griffin, K. 2010. Remote Desktop Services Resource Kit. Washington: Microsoft Press (134-142, 512-515)

Remote Desktop Services -testiympäristön IP-osoitteet:

Virtuaalikone 1:

Hennex-AD	192.168.0.10 255.255.255.0
DNS	192.168.0.10
DHCP	pooli 192.168.0.14 – 192.168.0.25

Virtuaalikone 2:

WIN-STAR	192.168.0.12 255.255.255.0
(RD Session Host)	

Virtuaalikone 3:

WebGateway	192.168.0.13 255.255.255.0
(RD Web Access ja RD Gateway)	

Fyysiset laitteet:

HP-palvelin (ESXi) 10.0.0.10 255.255.255.0

Hallinta-työasema 10.0.0.2 255.255.255.0

Ulkoverkon työasema (VLAN 20):

WIN-7 työasema (workgroup) 192.168.2.4 255.255.255.0

Domain Controllers asennus

Asennetaan palvelimelle:

Microsoft Server 2008 R2 (64bit)

Luodaan uusi domain controller:

1. Koneen IP:ksi määritetään 192.168.0.10/24.
2. DNS-osoitteeksi 192.168.0.10.
3. Suoritetaan run toiminnolla dcpromo.
4. Luodaan uusi metsä ja nimetään se “testilab.local”.
5. Valitaan metsän toimintatasoksi Windows Server 2008.
6. Varmistetaan, että DNS on valittu käyttöön ja painetaan “Yes” luomalla delegointi DNS-palvelimille.
7. Hyväksytään tietokanta-, lokitiedostojen- ja SYSVOL-asetukset oletuksin.
8. Määritetään salasanaksi “password1!”.
9. Hyväksytään yhteenveto tehdyistä asetuksista ja käynnistetään kone uudelleen asetusten voimaantulemiseksi.
10. Luodaan toimaalueelle käyttäjät “rryti” ja “mkoivisto”. Käyttäjien luominen tehdään siirtymällä seuraavasti Start → Administrator → ja klikataan “Active Directory Users and Computers”.
11. Laajennetaan testilab.local kuvaketta, painetaan hiiren oikealla napilla “Users” ja valitaan “New → User”.
12. Lisätään kenttiin henkilötiedot ja salasana, lopuksi painetaan “Next” ja “Finish”.

RD Session Host asennus ja konfiguraatiot:

1. Asennetaan Windows Server 2008 R2.
2. Konfiguroidaan TCP/IP asetukset.
3. Liitetään WIN-STAR palvelin testilab.local toimialueeseen.
4. Asennetaan RD Session Host rooli.

Liitetään STAR-RDSH palvelin testilab.local toimialueeseen:

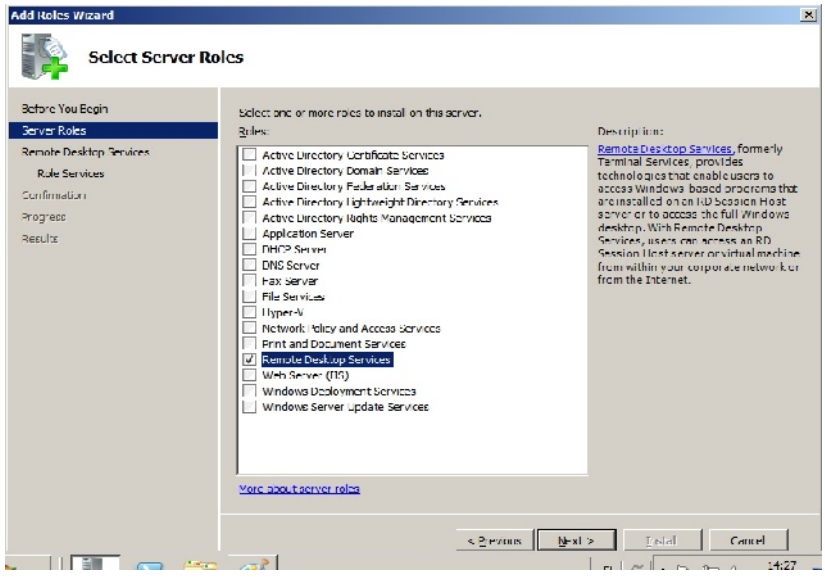
1. Kirjaudutaan STAR-RDSH palvelimelle järjestelmänvalvojan tunnuksilla.
2. Käynnistetään ”Start”, valitaan hiiren oikealla napilla ”Computer” ja liukuvalikosta ”Properties”.
3. Valitaan “Computer name, domain and workgroup settings” alta, “Change settings”.
4. Valitaan Computer Name kohta, klikataan “Change”.
5. Computer Name/Domain Changes valintaikkunassa, valitaan ”Domain” ja lisää domain osoite. Testiympäristössä se on: testilab.local
6. Klikataan ”More”, ja Primary DNS suffix of this computer kenttään lisätään myös domain nimi eli: testilab.local
7. Klikataan ”OK ”ja uudelleen ”OK”.
8. Seuraavaksi se pyytää järjestelmänvalvojan tunnuksia ennen kuin hyväksytään toimialueeseen liittyminen. Tämän jälkeen tietokone käynnistetään uudelleen, jolloin asetukset tule voimaan.

RD Session Host -roolin asennus

RD Session Host -roolin asennus suoritetaan palvelimen Server Manager -hallintatyökalulla. Hallintatyökalu löytyy palvelimelta, Start-Administrative Tools-Server Manager. Roolin asentaminen aloitetaan valitsemalla ”Add roles”.

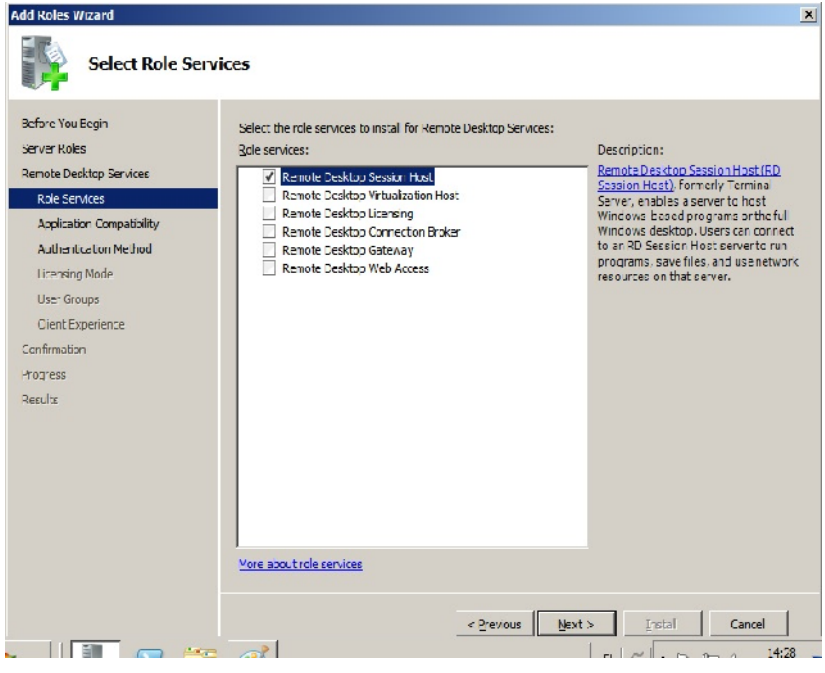
Ennen RD Session Host roolin asentamista tulee kiinnittää huomiota siihen, että palvelimelle ei ole asennettu Active Directory Domain Services -roolia entuudestaan. Tämä on otettava huomioon tietoturvasyistä.

Remote Desktop Services löytyy roolilistasta, jossa on sen lisäksi 16 muuta roolia. Valitaan listalta asennettavaksi Remote Desktop Services -rooli (kuva 1).



Kuva 1. Valitaan listalta Remote Desktop Services.

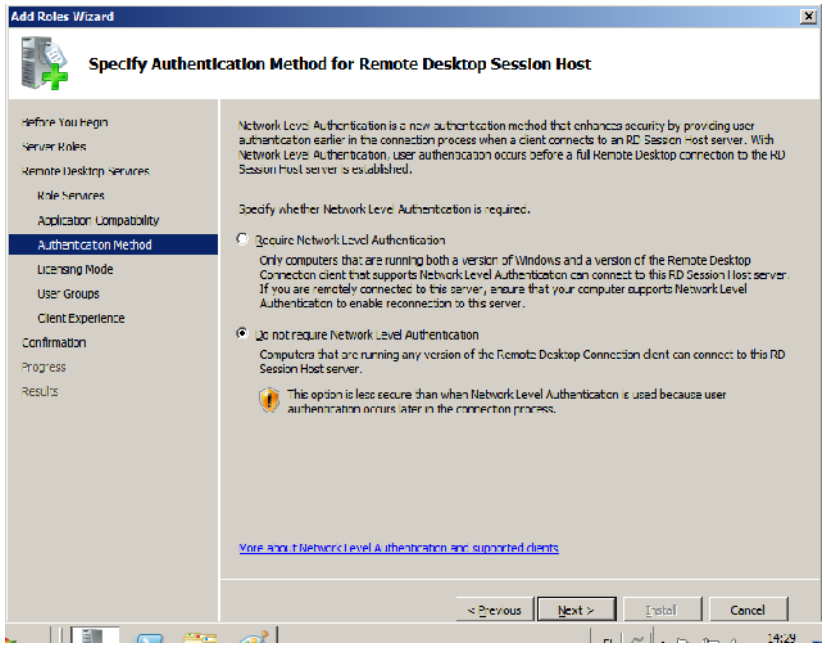
Remote Desktop Services sisältää kuusi erilaista roolia. Etäpöytäroolien asentaminen tässä opinnäytetyössä on jaettu kahteen osaan. Testiympäristöön otetaan käyttöön Remote Desktop Session Host -rooli omalle virtuaalikoneelle sekä RD Web Access ja RD Gateway kummatkin roolit samalle virtuaalikoneelle. Ensimmäiseksi asennetaan RD Session Host -rooli (kuva 2).



Kuva 2. Valitaan Remote Desktop Session -rooli asennettavaksi.

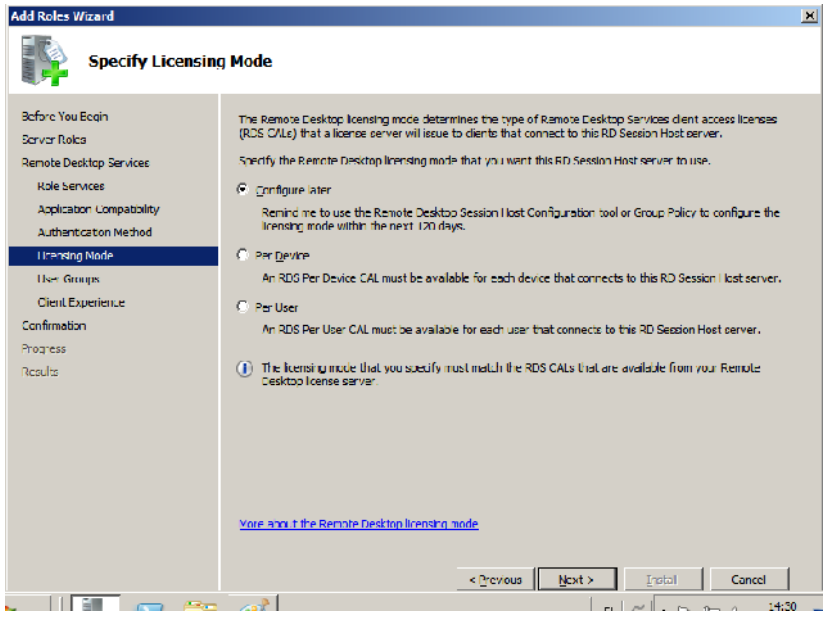
Etäpöytäpalvelun asennuksen aikana saattaa tulla varoitus, joka varoittaa palvelimelle entuudestaan asennetuista ohjelmista. Tällöin olemassa olevat ohjelmat eivät välttämättä toimi Remote Desktop Services -roolien asennusten jälkeen.

Autentikointimetodiksi valitaan NLA (Network Level Authentication), jonka tarkoituksena lisätä turvallisuutta käyttäjien kirjautuessa RD Session Host -palvelimelle (kuva 3). NLA:ta käyttöön otettaessa tietokoneiden käyttöjärjestelmiksi vaaditaan Windows 7, Vista SP1 tai XP SP3.



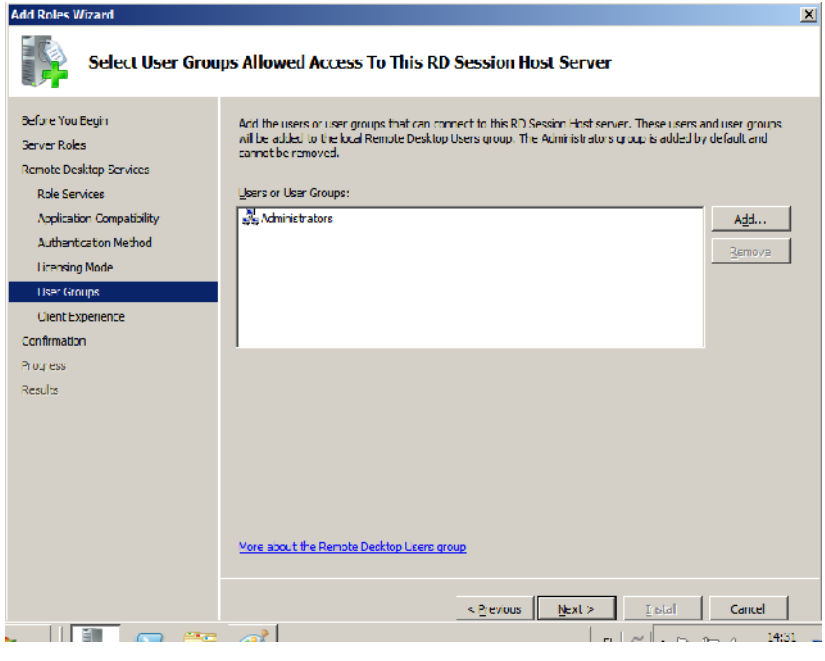
Kuva 3. Valitaan NLA-autentikointi käyttäjille

Asennus jatkuu lisensointimallin valinnalla (kuva 4). Vaihtoehtoisina lisensointimalleina etätyöpalvelulle on joko laite- tai käyttäjäkohtainen lisenssi. Jos ei vielä tiedä kumman lisensointimallin haluaa valita, voi sen määritellä myöhemmin. Tässä tapauksessa jätetään lisensointityypin valinta myöhemmäksi, koska kyseessä on vain testiympäristö. Testiympäristöä voi käyttää 120 päivää ilmaiseksi, jonka jälkeen lisensointimalli on viimeistään valittava.



Kuva 4. Laite- tai käyttäjäkohtaisen lisensointityypin valinta.

Lisensointivalinnan jälkeen valitaan ne käyttäjät joilla on pääsy RD Session Host –palvelimelle (kuva 5). Palvelimelle voivat kirjautua ne käyttäjät, jotka on lisätty Remote Desktop Users -ryhmään. Oletuksena etäpalvelun käyttäjiksi on valittu Administratorin ryhmä. Tämä kohta vaatii erityistä tarkkuutta jos jokin lisensointimalli on valittuna, koska lisenssien määrä laitetta tai käyttäjää kohti on rajoitettu eikä kaikilla käyttäjillä ole välttämättä tarvetta käyttää etäpöytäpalvelua.

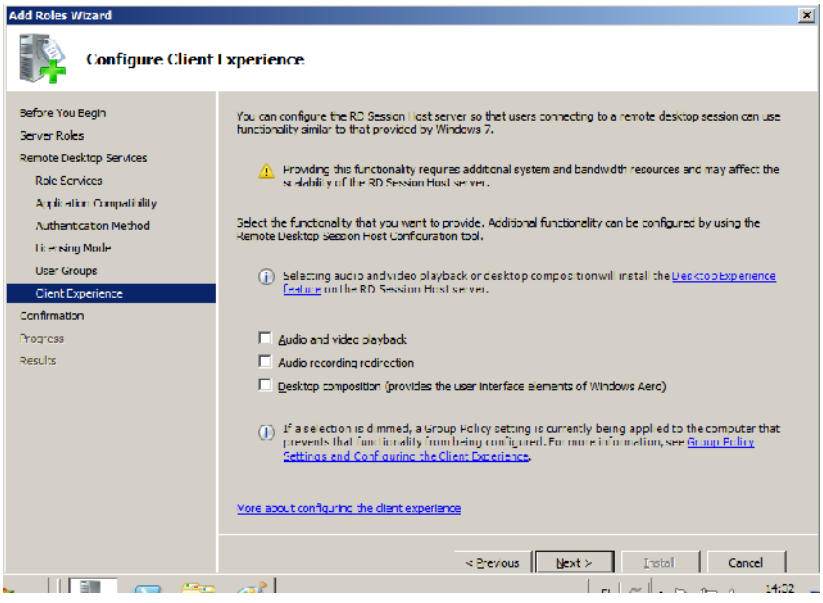


Kuva 5. Käyttäjien ja ryhmien lisääminen RD Session Host -palvelimelle.

Etäpöytäpalveluiden käyttäjät tulee lisätä Remote Desktop Users -ryhmään Active Directory Users and Computers -palvelussa.

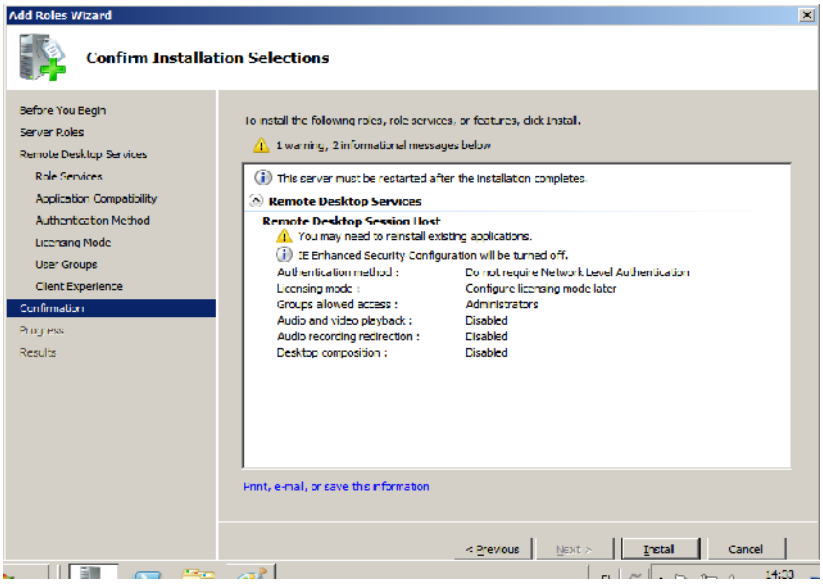
Toinen tapa on rajoittaa käyttäjien pääsyä, luomalla security group, joka voidaan nimetä vaikka Oppilaat RDS käyttäjät. Käyttäjät lisätään RD Session Host palvelimella security groupiin ja lisätään Oppilaat RDS käyttäjät -ryhmä AD:ssa Remote Desktop Users -ryhmään.

Sopivien käyttäjien valinnan jälkeen, painetaan ”Next”. Etäpöytäyhteyden lisäksi voidaan valita ääni- ja videotoimintoja (kuva 6). Näitä Windows aero-toimintoja käytetään myös Vistassa ja Windows 7:ssa. Nämä toiminnot ovat tulleet uutena Windows Server 2008 R2 mukana. Toiminnot ottaessa käyttöön on huomioitava, että toimintojen valinta vaikuttaa yhteyden laatuun.



Kuva 6. Ääni- ja videotoimintojen valinta.

Asennusvaiheen viimeisessä kohdassa vahvistetaan valittujen asetusten voimaantulo. Ruudulla on näkyvillä lista aikaisemmin tehdyistä asetuksista. Tarkistetaan, että kaikki asetukset ovat oikein ja valitse ”Install” (kuva 7).



Kuva 7. Yhteenveto tehdyistä asetuksista, aloitetaan asennus painamalla “Install”.

Asennuksen jälkeen tulee ilmoitus asennuksen onnistumisesta. Painetaan ”Close” ja sen jälkeen käynnistetään palvelin uudelleen.

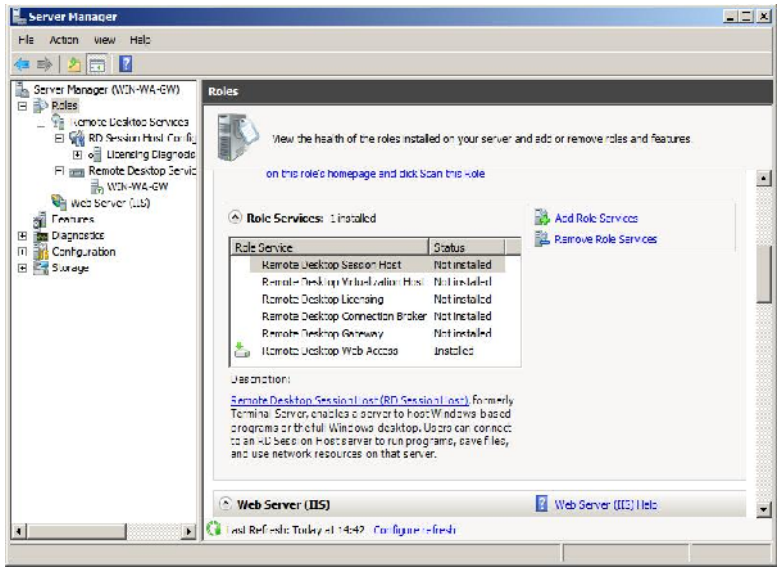
Toimialueen käyttäjän lisääminen Remote Desktop Users ryhmään:

1. Kirjaudutaan RD Session Host (WIN-STAR) palvelimelle administrator tunnuksilla.
2. Klikataan “Start”, valitaan “Administrator Tools” ja “Computer Management”.
3. Laajennetaan kohta Local Users and Groups, ja klikataan “Groups”.
4. Remote Desktop Users kohdalla painetaan hiiren oikeata nappia ja valitaan liukuvalikosta ”Add to Groups”.
5. Remote Desktop Users -valintaikkunassa, klikataan ”Add”.
6. Select Users, Computers, Services Accounts, or Groups -valintaikkunassa,lisätään Enter the object names to select -kenttään, toimialueen käyttäjän nimi esim. rryti ja klikataan “OK”.
7. Lopuksi klikataan “OK”.

RD Web Access ja RD Gateway -roolien asennus:

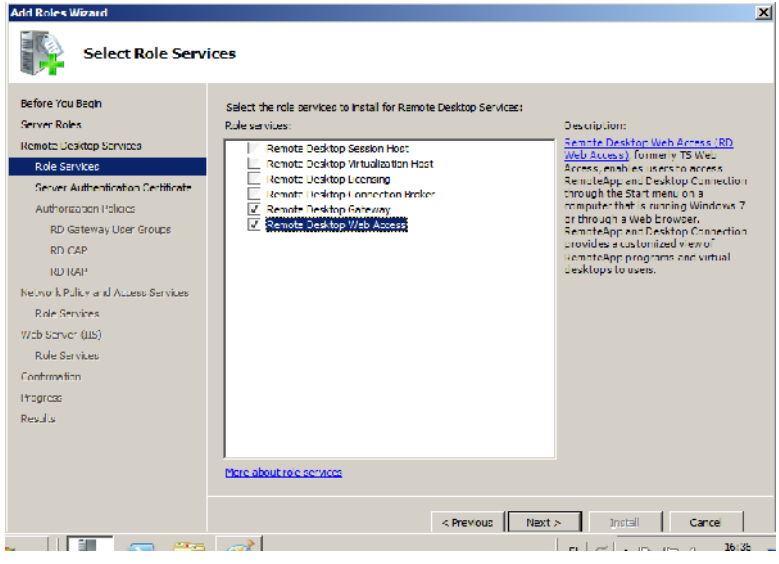
1. Asennetaan Windows Server 2008 R2
2. Konfiguroidaan TCP/IP asetukset.
3. Liitetään webgateway-palvelin testilab.local toimialueeseen.
4. Asennetaan RD Web Access ja RD Gateway roolit.

RD Web Access ja RD Gateway -roolien asentaminen aloitetaan Server Manager -hallintatyökalulla. Asennus käynnistetään valitsemalla kohta ”Add Role” (kuva 8).



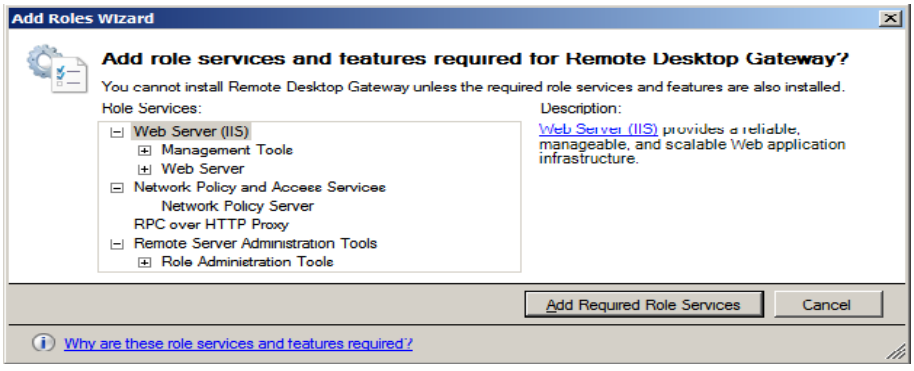
Kuva 8. Server Manager -hallintatyökalu, josta roolien asennus aloitetaan.

Valitaan asennettaviksi rooleiksi RD Web Access ja RD Gateway (kuva 9).



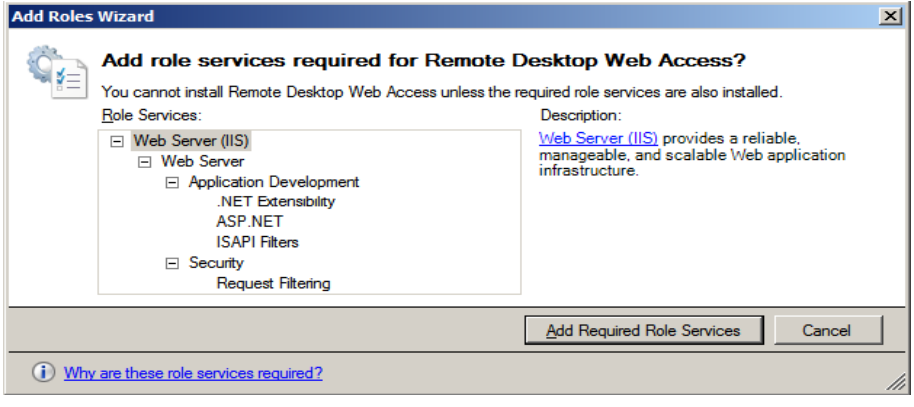
Kuva 9. Valitaan asennettaviksi rooleiksi RD Gateway ja RD Web Access.

Roolivalintojen yhteydessä ruudulla tulee näkyville pieni ikkuna, jossa kerrotaan mitä palveluita RD Gateway tarvitsee. Hyväksytään kaikki lisäpalvelut oletuksin Add Required Role Services (kuva 10).



Kuva 10. RD Gatewayn lisäpalvelut.

Samankaltainen ilmoitus tulee, kun valitaan RD Web Access. Otetaan lisäpalvelut käyttöön “Add Request Roles Services (kuva 11)



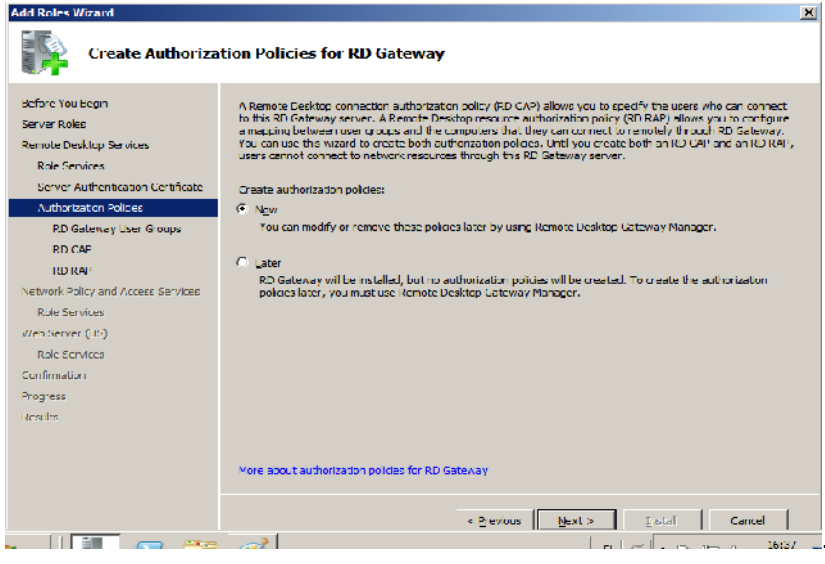
Kuva 11. RD Web Access:n lisäpalvelut.

Seuraavaksi määritellään SSL-salaus (kuva 12). Luodaan tässä tapauksessa self-signed certificate, joka on tarkoitettu testiympäristön käyttöön. Tilanteesta riippuen autentikointiasetusten määrittäminen voidaan jättää myöhempään ajankohtaan.

Kuva 12. Salausvarmenteen valitseminen.

Testitarkoituksessa voidaan käyttää Self-signed -sertifikaattia, mutta sen käyttöä ei suositella tuotantokäytössä. (Anderson & Griffin 2010, 511). Varmenne tarvitaan aina etäpalvelua käyttäviin työasemiin.

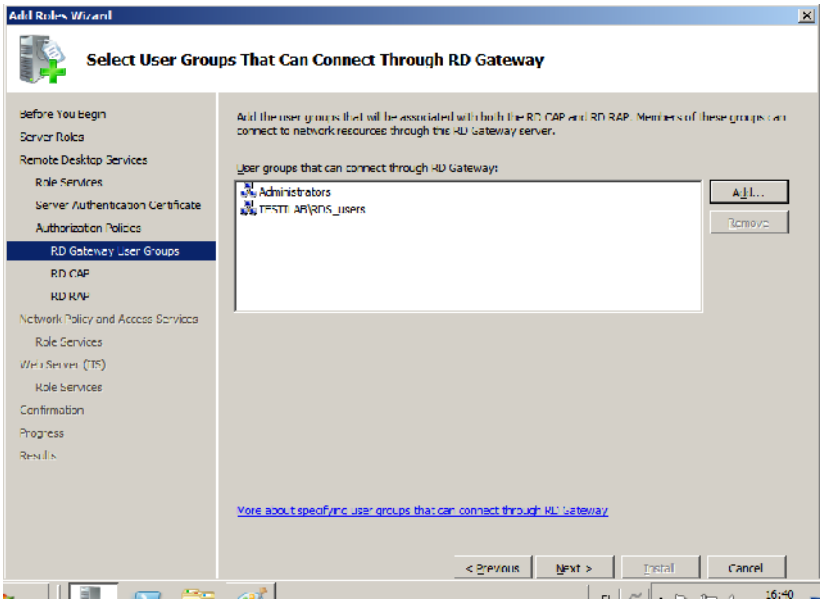
SSL-asetusten jälkeen määritellään auktorisointiasetukset (kuva 13). Vaihtoehtoina on tehdä määritykset joko heti tai myöhemmin. Auktorisointisäännöt voidaan määritellä myöhemmin RD Gateway Management konsolissa. Tässä tapauksessa valitaan vaihtoehto ”now”.



Kuva 13. Auktorisointisääntöjen määrittäminen.

RD Gateway Users Groups- ikkunassa lisätään ne paikalliset käyttäjät tai toimialueen käyttäjät, joilla on oikeus kytkeytyä RD Gateway palvelimeen. Tämän jälkeen tehdään auktorisointisäännöt kahdelle eri tyypille, RD CAP:lle ja RD

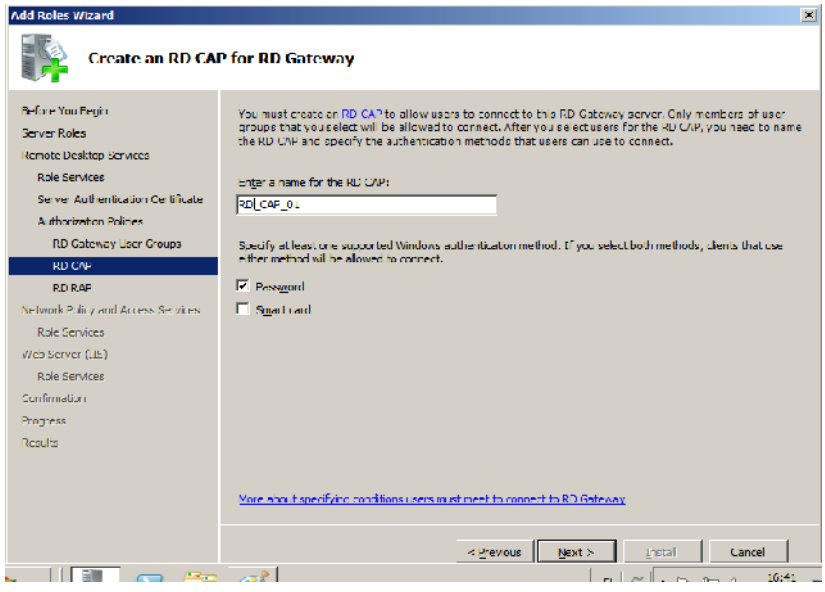
RAP:lle. Ensimmäisessä tapauksessa määritellään ne käyttäjät, jotka saavat kytkeytyä RD Gateway palvelimeen, toisessa määritellään ketkä saavat oikeuden käyttää sisäverkon resursseja. Kuvassa 14 näkyy ”Add” -toiminnolla haettu testilab-toimialueen RDS_users-ryhmä.



Kuva 14. Valitaan ryhmät joilla on oikeus kytkeytyä RD Gatewayn kautta etäpöytäjärjestelmään.

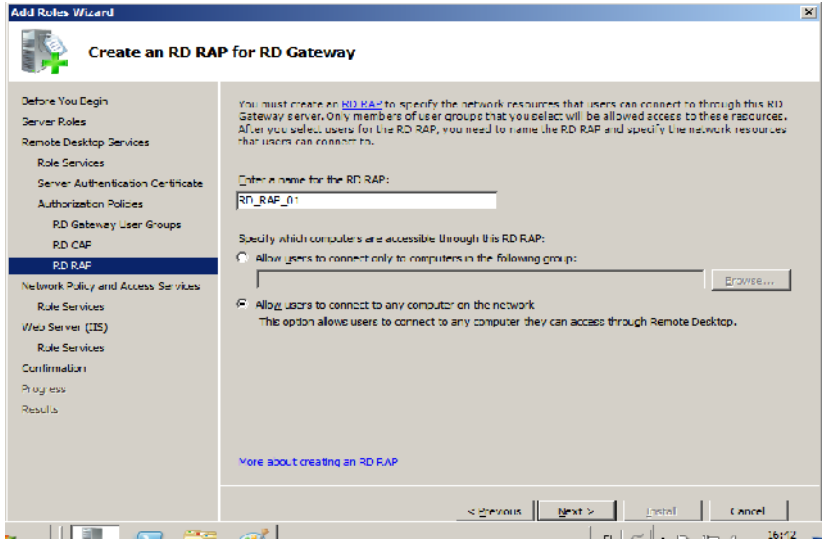
Jos etäpöytäratkaisua rakennetaan tuotantoympäristöön, on syytä olla tarkkana, keitä hyväksytään käyttämään RDS-palveluita lisenssit huomioon ottaen. Käyttöoikeudet etäpalvelun käyttöön annetaan vain niille, joilla on välttämätön tarve ja kyseiset käyttäjät kannattaa lisätä aktiivihakemistossa Remote Desktop Services -ryhmään. Tällä tavalla helpotetaan käyttöoikeuksien hallintaa.

Seuraavaksi määritetään auktorisointikäytännöt. Ensimmäisenä tehdään määritykset RD CAP:lle. Annetaan nimi kyseiselle auktorisointityypille, esimerkiksi RD_CAP_01 ja lisätään käyttäjät, joille annetaan oikeus kirjautua RD Gateway palvelimelle (kuva 15). Samassa yhteydessä valitaan Windows autentikointimetodi, joka esitetään kirjauduttaessa RD Gateway palvelimelle. Vaihtoehtoina ovat salasana tai älykortti, tarpeen tullen mukaan voidaan valita molemmat.



Kuva 15. RD CAP -auktorisointikäytännön nimeäminen.

Tehdään määritykset RD RAP:lle (kuva 16). Annetaan nimi esim. RD_RAP_01 ja lisätään erikseen ne käyttäjäryhmät, joilla on oikeus käyttää sisäverkon resursseja tai annetaan kaikille käyttäjille lupa käyttää niitä.



Kuva 16. RD CAP -auktorisointikäytännön nimeäminen.

Loppuvaiheessa tulee ikkuna, jossa kerrotaan IIS palvelusta. Painetaan ”Next”. Vahvistetaan asennettava rooli painamalla Install.

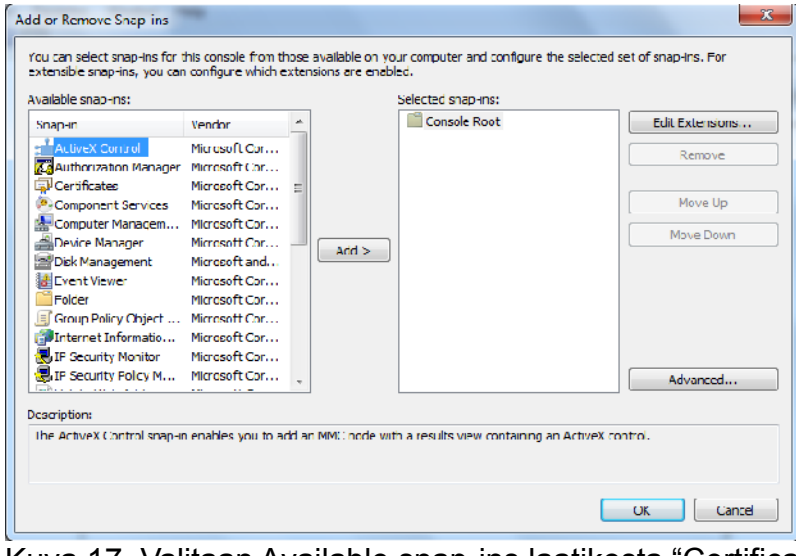
RD Web Access ja RD Gateway roolien konfigurointi:

Itseallekirjoitetun SSL-sertifikaatin luominen RD gateway palvelimella:

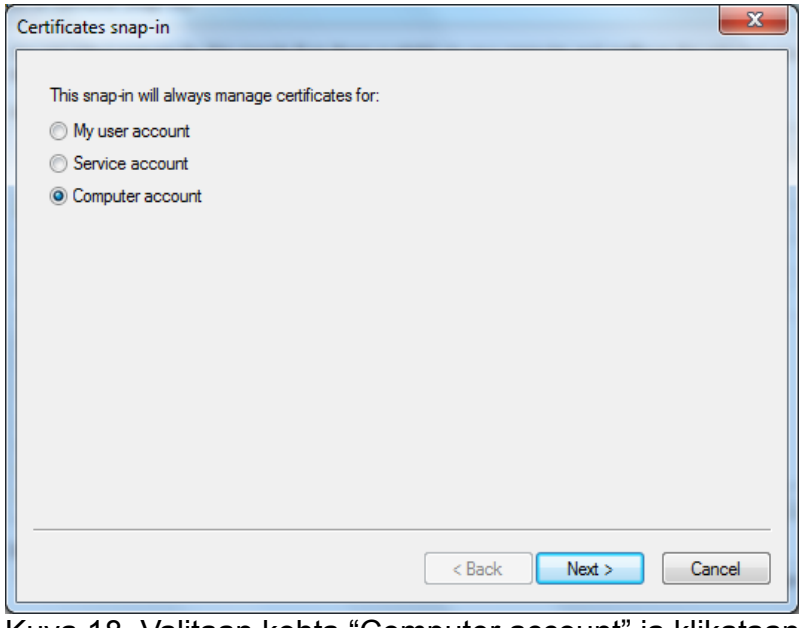
1. RD Gateway palvelimella klikkataan ”Start” → ”Run”, kirjoitetaan mmc ja klikataan ”OK”.
    a. Avataan yläpalkista File ja klikataan ”Add/Remove Snap-in”.
    b. Add or Remove snap-ins valintaikkunassa, Available snap-ins listalla, klikataan kohtaa ”Certificates” ja sitten klikataan ”Add”.
    c. Certificates snap-in valintaikkunassa, klikataan ”Computer Account” ja sen jälkeen painetaan ”OK”.
    d. Select Computer valintaikkunassa, klikkataan “Local computer (the computer this console is running on)” ja sitten klikataan “Fin ish”.
2. Certificate snap-in konsolissa, navigoidaan Certificates\Personal\Certificates ja valitaan lisätty sertifikaatti hiiren oikealla painikkeella ja valitaan All Tasks → Export.
3. Welcome to the Certificate Export Wizard sivulla, klikataan “Next”.
4. Export Private Key sivulla, valitaan Yes kohdassa “export the private key” ja sitten klikataan “Next”.
5. Export Private Format sivulla tarkistetaan, että Personal Information Exchange PKCS #12(.PFX) on aktivoitu. Rastitetaan kohta “Include all certificates in the certification path if possible” ja sitten klikataan “Next”.
6. Salasana sivulla, kirjoitetaan salasanaksi 123 ja klikataan ”Next”.
7. File to Export sivulla, File name kentässä, klikataan “Browser”.
8. Save as valintaikkunassa, lisätään nimi esim. Seuraavassa muodossa RDG-SRV ja sitten tallennetaan tiedosto.
9. File to Export sivulla, painetaan “next”.
10. Sertifikaatti on valmis, painetaan ”OK”.
11. Kopioidaan juuri luotu RD Gateway server sertifikaatti asiakaspäätteille.

SSL-sertifikaatin asentaminen asiakaspäätteelle:

1. Kirjaudutaan asiakaskoneelle administrator tunnuksilla.
2. Käynnistetään Certificates snap-in konsoli, avaamalla ”Start” → ”Run” ja kirjoitetaan mmc ja sitten painetaan ”OK”.
3. Avataan yläpalkista ”File” ja klikataan ”Add/Remove Snap-in”.
4. Valitaan Available snap-ins laatikosta “Certificates” ja painetaan “Add” (kuva 17).
5. Certicates snap-in valintaikkunassa, valitaan kohta “Computer account” ja klikataan “Next” (kuva 18).

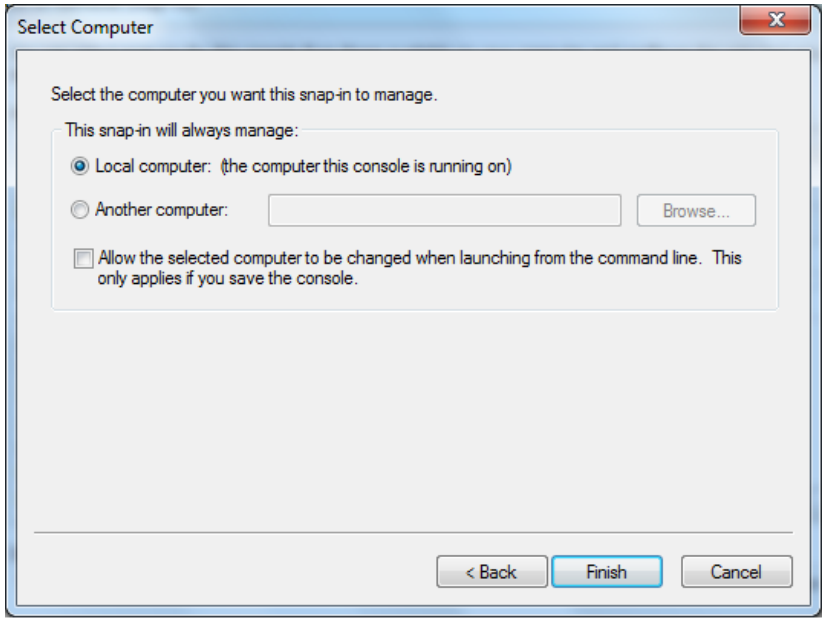


Kuva 17. Valitaan Available snap-ins laatikosta “Certificates” ja painetaan “Add”.



Kuva 18. Valitaan kohta “Computer account” ja klikataan “Next”.

6. Select Computer ikkunassa, valitaan kohta “Local computer: (the computer this console is running on)” ja lopuksi painetaan “Finish”. Add of Remove snap-ins valintaikkunassa klikataan “OK” (kuva 19).

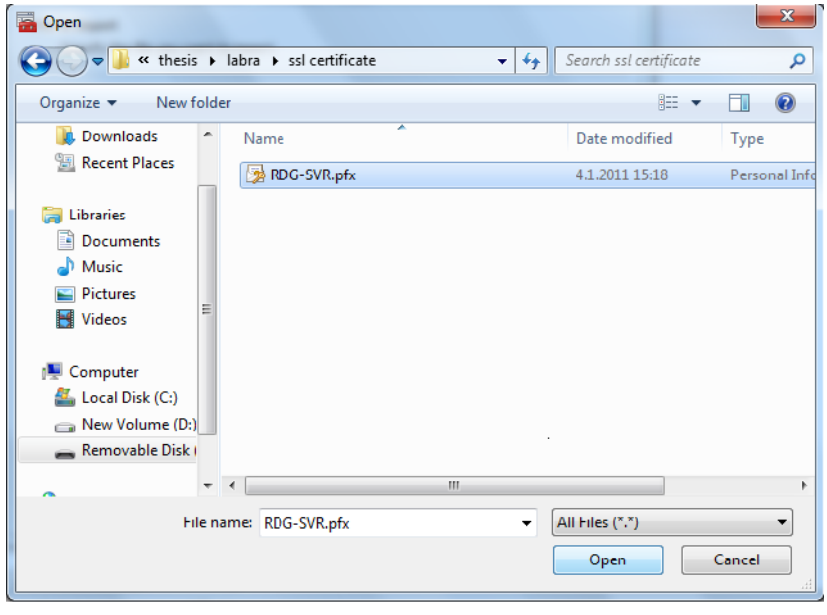


Kuva 19. Valitaan ”Local computer”.

7. Certificate snap-in konsolissa navigoidaan Certificates\Personal ja klikataan hiiren oikeata nappia ”Personal kansion” kohdalla ja valitaan liukupaneelista ”All Tasks” → ”Import”.
8. Certificate Import Wizard ikkunassa jatketaan painamalla “Next” (kuva 20).

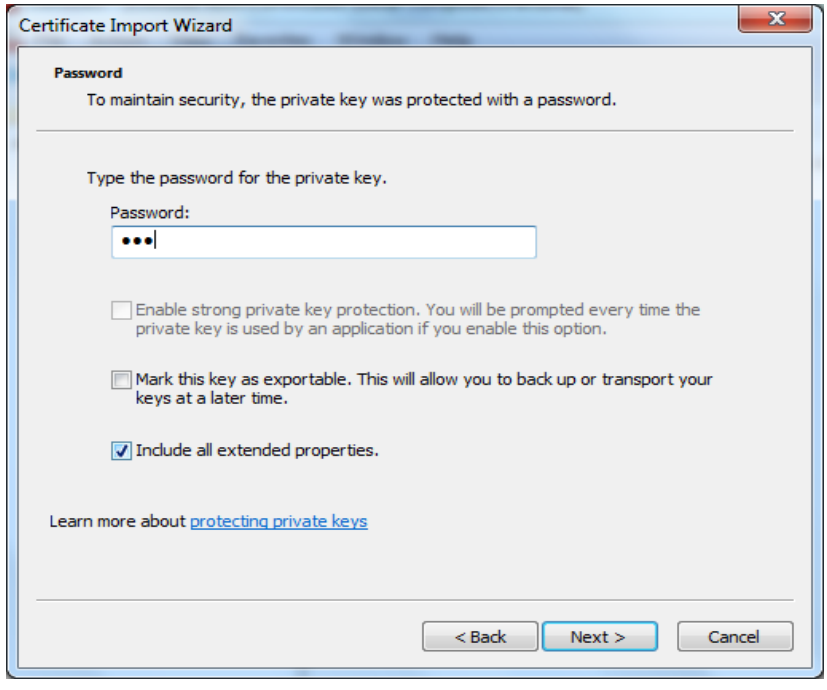
Kuva 20. Certificate Import Wizard ikkunassa jatketaan painamalla “Next”.

9. Haetaan RD Gatewayn SSL-sertifikaatti ja valitaan tiedostotyyppi valikosta All Files(*.*) (kuva 21).



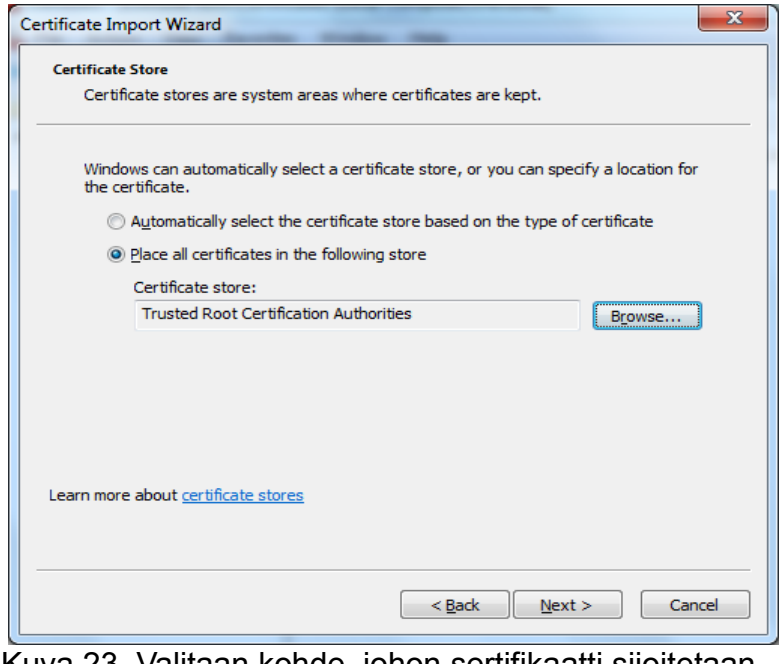
Kuva 21. RD Gatewayn SSL-sertifikaatti.

10. Lisätään sertifikaattiin määritelty salasana: 123 ja laitetaan rasti kohtaan “Include all extended properties” (kuva 22).



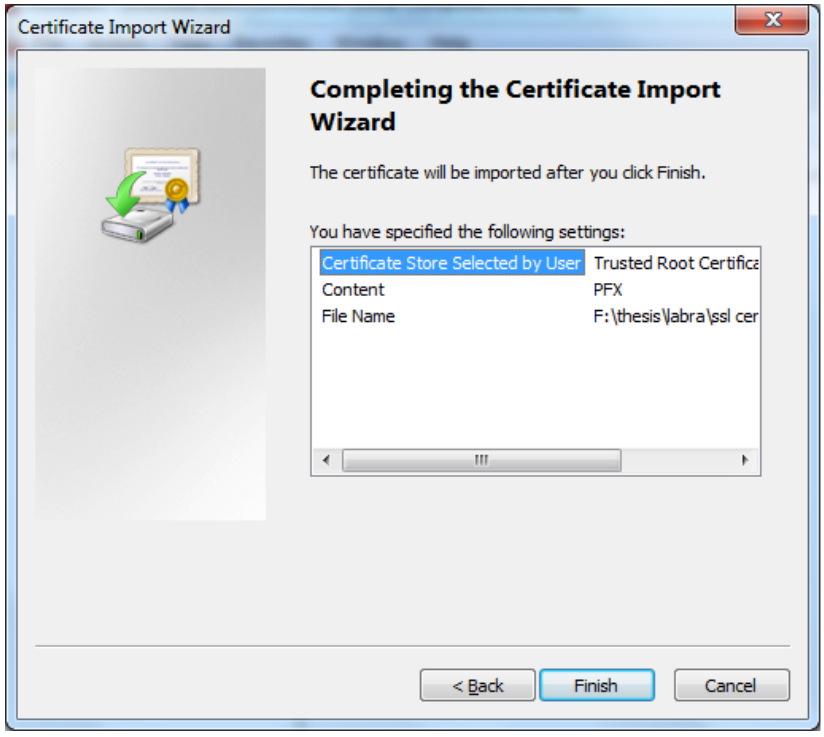
Kuva 22. Sertifikaatin salasana.

11. Certificate Store sivulla sijoitetaan sertifikaatti varastoon: Trusted Root Certification Authorities ja painetaan “Next” (kuva 23).



Kuva 23. Valitaan kohde, johon sertifikaatti sijoitetaan.

12. Lopuksi tulee näkyville yhteenveto sertifikaatin asennuksesta. Painetaan ”Finish” (kuva 24).



Kuva 24. Yhteenveto sertifikaatin asennuksesta.

RD Web Access -konfigurointi:

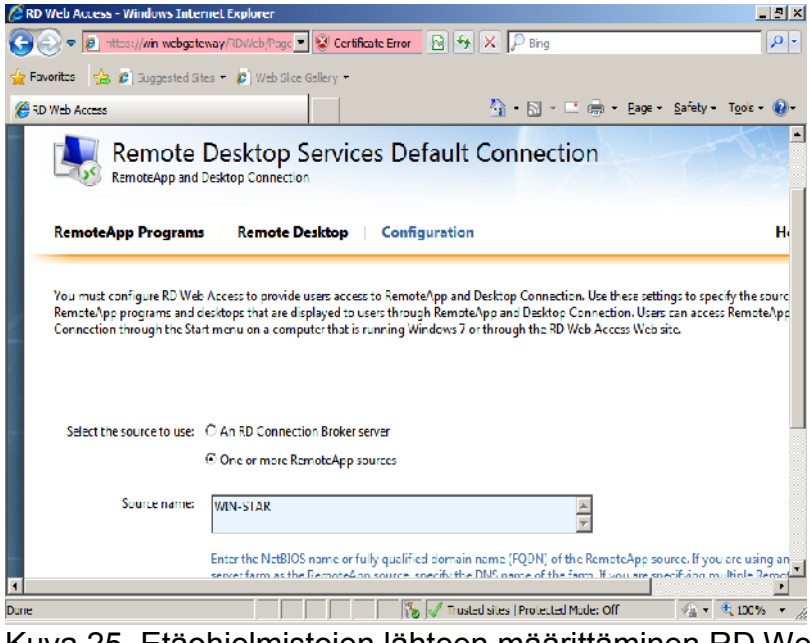
RD Web Access asennuksen jälkeen tehdään muutamia asetuksia, ennen kuin toimialueen käyttäjä voi suorittaa etäpalveluja internetselaimen kautta. Ensinnäkin täytyy määritellä asetukset, jotta RD Web Access -palvelin voi kytkeytyä RD Session Host -palvelimelle, jossa etäohjelmat sijaitsevat. Asetukset tehdään lisäämällä RD Web Access -palvelin RD Session Host palvelimessa TS Web Access Computers local ryhmään. Start → Administration Tools → Computer Management. Computer Management laajennetaan ikkuna Local Users and Groups ja valitaan Groups. Group-kansiosta löytyy TS Web Access Computers kansio. Kaksoisklikataan sitä. TS Web Access Computers asetuksissa voi määritellä ketkä voivat käyttää RD Web Access -roolin jakamia palveluita.

Edellä tehtyjen asetusten lisäksi määritetään RD Web Access palvelimella lähde josta saadaan etäohjelmat ja täysi etäpöytäyhteys käyttöön. Avataan IE-selain ja kirjoitetaan osoitekenttään https://webservername/rdweb. Tämän jälkeen esille tulee kirjautumisruutu. Kirjaudutaan administrator-tunnuksilla. Oletuksena pitäisi avautua Configuration välisivu. Avautuneella sivulla lisätään RD

Session Host server, joka jakaa etäohjelmat ym. Lisätään etäohjelmalähde seuraavassa muodossa: **win-star.testilab.local.**

Testiympäristössä RD Web Access palvelimen konfigurointi:

1. Selaimen osoitekenttään kirjoitetaan https://win-webgateway/rdweb
2. Remote Desktop Services Default Connection käyttöliittymässä kirjaudutaan pääkäyttäjän tunnuksilla: administrator ja password1!
3. Valitaan käyttöliittymässä välilehti ”Configuration” (kuva alla).
4. Valitaan lähde “One or more RemoteApp sources” ja lisätään kenttään etäohjelmia ja työpöytiä jakavan palvelimen eli kyseessä on RD Session Host palvelin nimellä WIN-STAR (kuva 25).
5. Asetuksen jälkeen etäohjelmien pitäisi tulla näkyviin “RemoteApp Programs” välilehdellä.

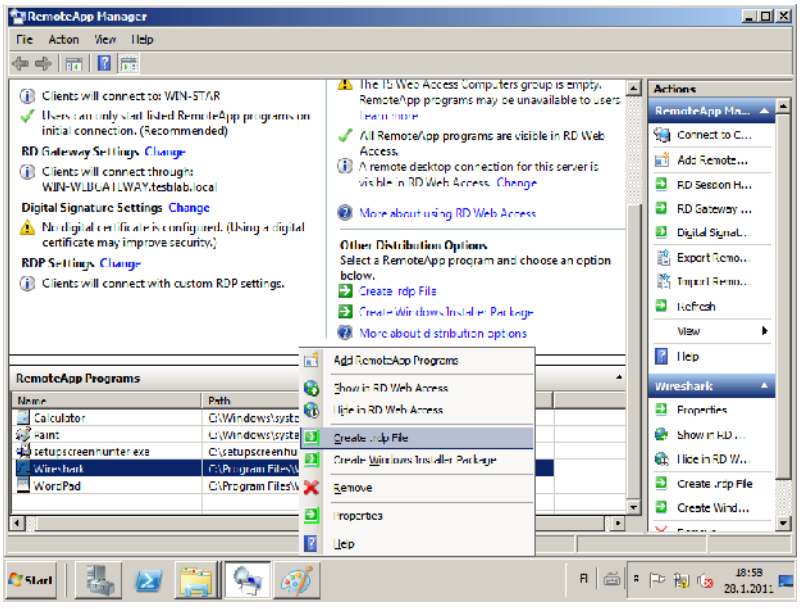


Kuva 25. Etäohjelmistojen lähteen määrittäminen RD Web Access -konfiguraatiossa.

RDP-tiedoston luominen

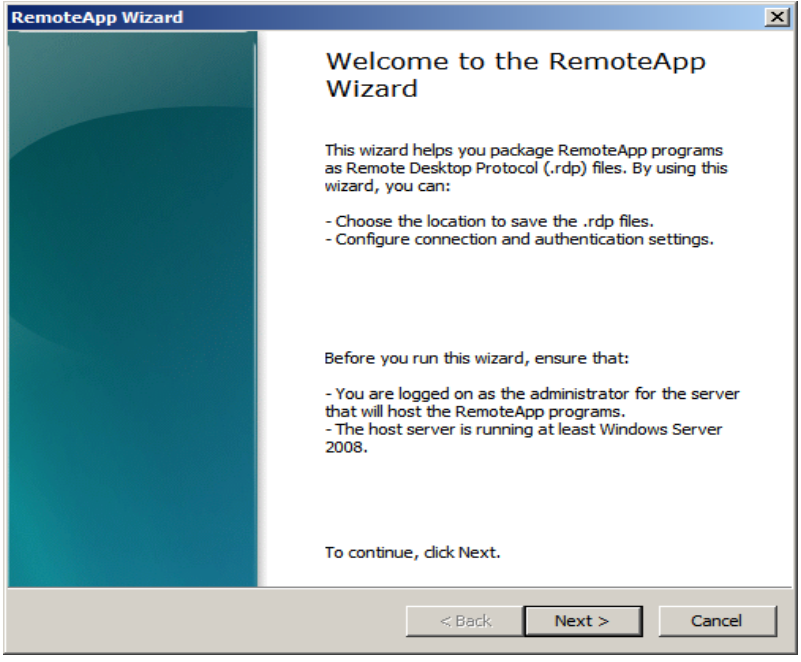
RDP-tiedoston luominen voidaan tehdä RD Session Host -palvelimella RemoteApp Managerissa (kuva 26). Ensimmäiseksi haluttu ohjelma asennetaan palvelimelle ja lisätään se etäohjelma-listaan tai noudetaan etäohjelma-listalle jokin Windows-ohjelma.

RDP-tiedoston luonti käynnistetään siirtämällä hiiren osoitin alla olevan kuvan mukaisesti ohjelman päälle ja klikataan oikeanpuoleista nappia ja avautuneesta liukuvalikosta valitaan ”Create .rdp File”.



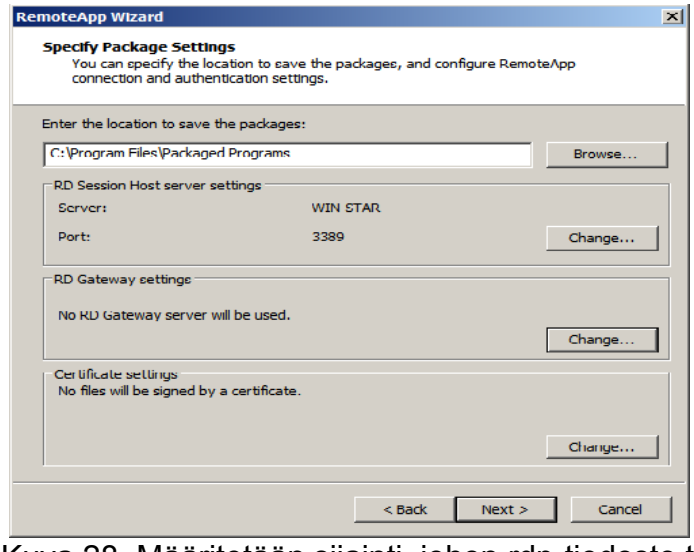
Kuva 26. RemoteApp Manager.

RemoteApp asennusohjelman käynnistyttyä painetaan ”Next” (kuva 27).



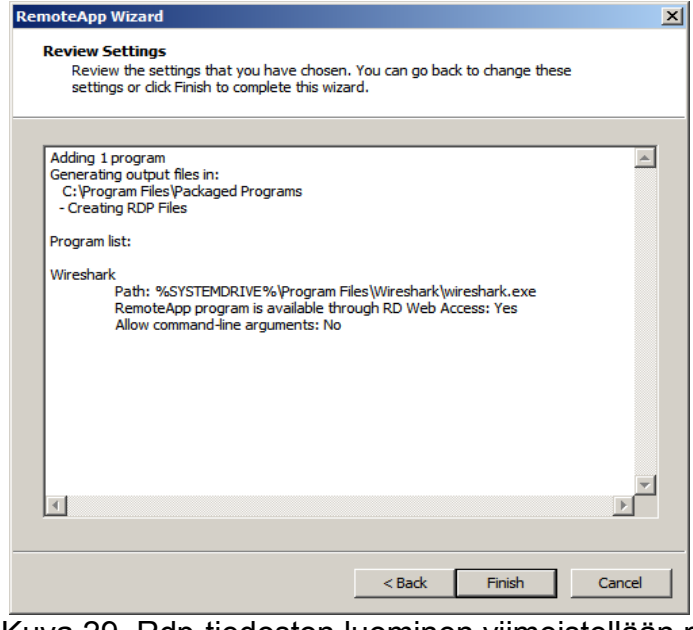
Kuva 27. .rdp-tiedoston luominen wizard-asennusohjelmalla.

Tässä kohdassa valitaan .rdp-tiedostolle haluttu sijainti, tarvittaessa muutetaan RD Session Host:n ja RD Gateway:n sekä sertifikaatin asetukset (kuva 28). Testiympäristössä RD Gatewayn asetukset jätettiin pois, jolloin asiakaspäätteellä käynnistetty rdp-tiedosto ei lähettänyt pyyntöjä RD Gatewayn kautta. Muutokset tehtiin ”Change” napin kautta.



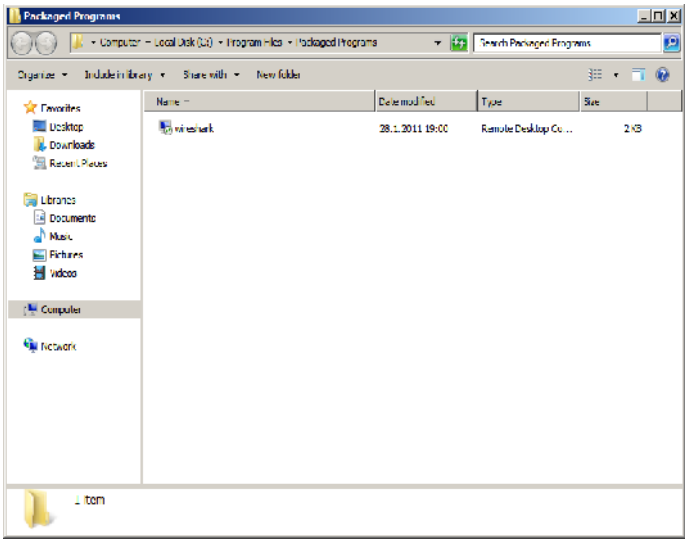
Kuva 28. Määritetään sijainti, johon.rdp-tiedosto tallennetaan.

Rdp-tiedoston luominen viimeistellään painamalla, ”Finish” (kuva 29).



Kuva 29. Rdp-tiedoston luominen viimeistellään painamalla, ”Finish”.

Välittömästi rdp-tiedoston luonnin jälkeen avautuu ikkuna, johon tiedosto tallennettiin (kuva 30). RDP-tiedosto löytyy samasta sijainnista toimialueen asiakaskoneelta. Tiedosto kopioidaan omalle työpöydälle ja se on valmis käytettäväksi.

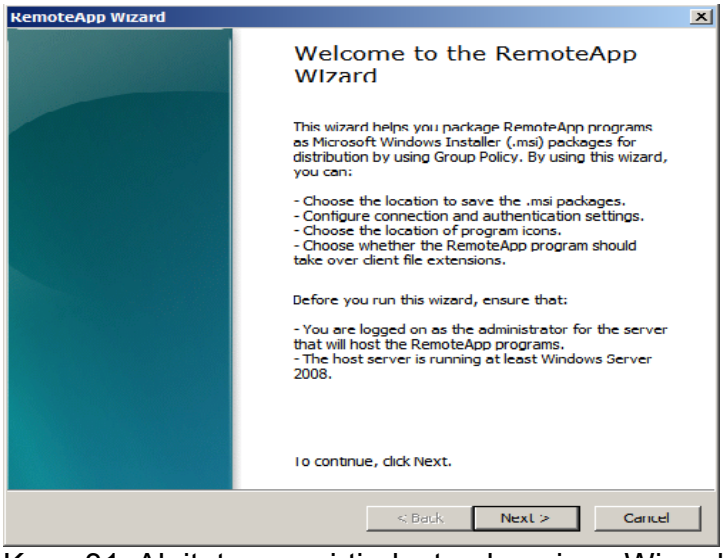


Kuva 30. rdp-tiedosto löytyy tallennetusta sijainnista.

MSI-tiedoston luominen

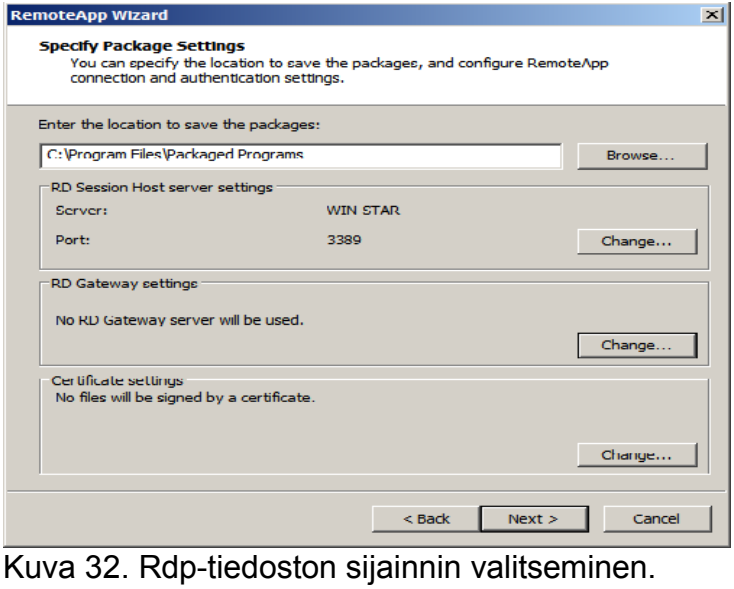
MSI-tiedoston luominen tehdään Remote Session Host palvelimella remoteApp managerissa. Ensiksi haluttu sovellus asennetaan palvelimeen tai poimitaan sovellus remoteApp:n ohjelmalistasta.

Käynnistetään MSI-tiedoston luonti RemoteApp Managerissa valitsemalla haluttu ohjelma etäohjelmalistalta, klikataan oikeanpuoleista nappia ohjelman kohdalla ja valitaan liukuvalikosta ”Create .msi File”. Wizard-asennusohjelman käynnistyttyä painetaan ”Next” (kuva 31).



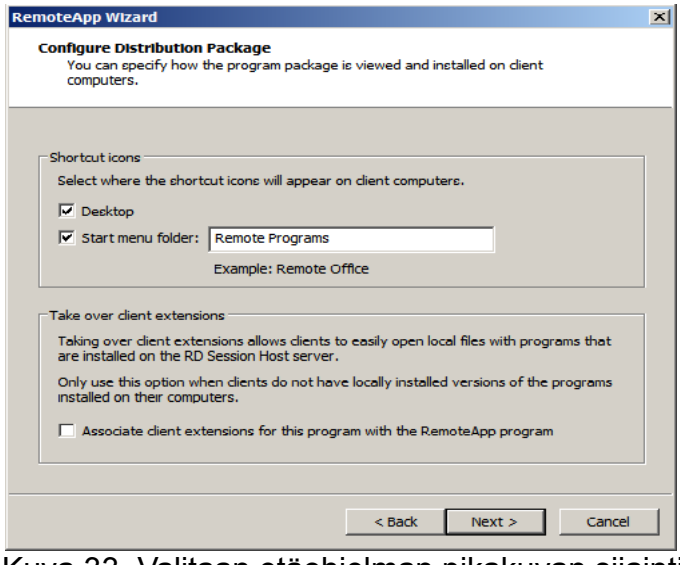
Kuva 31. Aloitetaan msi-tiedoston luominen Wizard-asennusohjelmalla.

Tässä kohdassa valitaan rdp-tiedostolle haluttu sijainti, tarvittaessa muutetaan RD Session Host:n ja RD Gateway:n –asetukset (kuva 32). Testiympäristössä RD Gatewayn asetukset jätettiin pois, jotta asiakaspäätteellä käynnistetty rdp-tiedosto ei lähettäisi pyyntöjä RD Gatewayn kautta. Muutokset tehtiin ”Change” napin kautta.



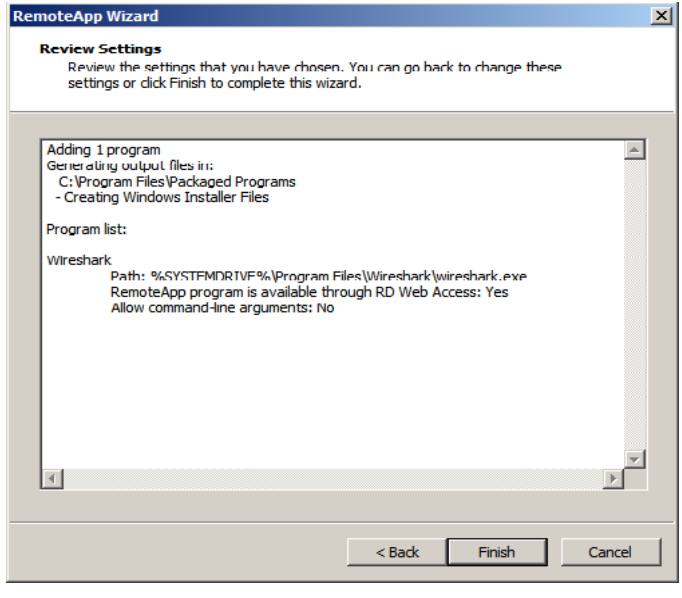
Kuva 32. Rdp-tiedoston sijainnin valitseminen.

Seuraavaksi valitaan etäohjelman pikakuvan sijainti, vaihtoehtoja ovat työpöytä ja käynnistä-valikko (kuva 33). Jos valitaan käynnistä-valikko, lisätään kansiolle nimi. Asennettavalle ohjelmalle voidaan tehdä tiedostolaajennus, jolloin asia-kaspäätteellä voidaan avata paikallinen tiedosto kyseisellä ohjelmalla. Tällöin rastitetaan asetukseen liittyvä kohta.



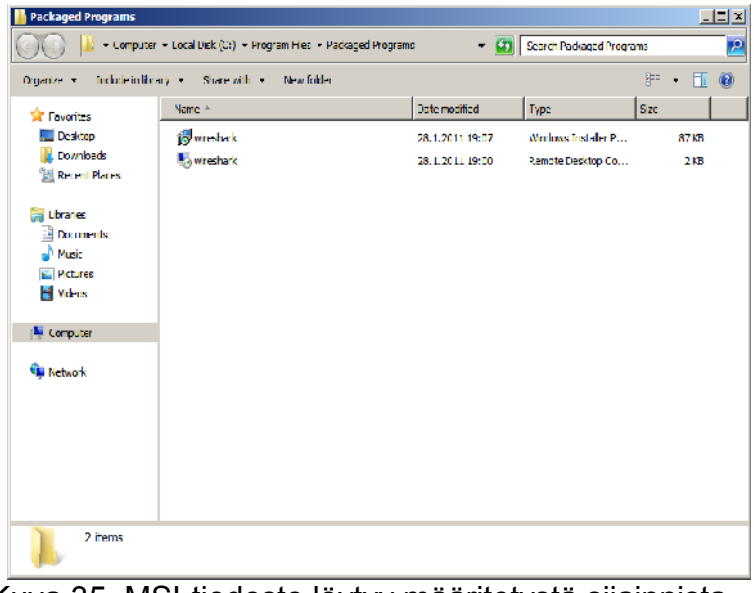
Kuva 33. Valitaan etäohjelman pikakuvan sijainti, vaihtoehtoja ovat työpöytä ja käynnistä-valikko.

MSI-tiedoston luominen viimeistellään painamalla ”Finish” (kuva 34).



Kuva 34. MSI-tiedoston luominen viimeistellään painamalla ”Finish”.

Välittömästi msi-tiedoston luonnin jälkeen avautui ikkuna johon tiedosto tallennettiin (kuva 35). msi-tiedosto löytyy samasta sijainnista toimialueen asiakaskoneelta. Tiedosto kopioidaan omalle työpöydälle ja se asennetaan, minkä jälkeen pikakuvakkeet esiintyvät työpöydällä ja käynnistä-valikossa.



Kuva 35. MSI-tiedosto löytyy määritetystä sijainnista.

VMware VIEW ASENNUS JA KONFIGURAATIOT

VMware View –testiympäristön asennuksissa käytettiin seuraavia lähdemateriaaleja:

ESX and vCenter Installation Guide.
http://www.VMware.com/pdf/vsphere4/r40/vsp_40_esx_vc_installation_guide.pd
Viitattu 15.12.2010.

VMware View Installation Guide.
http://www.VMware.com/pdf/view45_installation_guide.pdf Viitattu 15.12.2010

VMware View Administrator's Guide
http://www.VMware.com/pdf/view45_admin_guide.pdf Viitattu 15.12.2010

VMware View –testiympäristön IP-osoitteet:

Virtuaalikone 1 (Windows Server 2008 R2):

Hennex-AD 10.0.0.19 255.255.255.0

DNS 10.0.0.19 255.255.255.0

Virtuaalikone 2 (Windows Server 2008 R2):

vCenter 10.0.0.18 255.255.255.0

DNS 10.0.0.19

Virtuaalikone 3 (Windows Server 2008 R2):

VMware View (Connection server) 10.0.0.13 255.255.255.0

Virtuaalikone 4 (Windows 7):

WIN-7 10.0.0.15 255.255.255.0

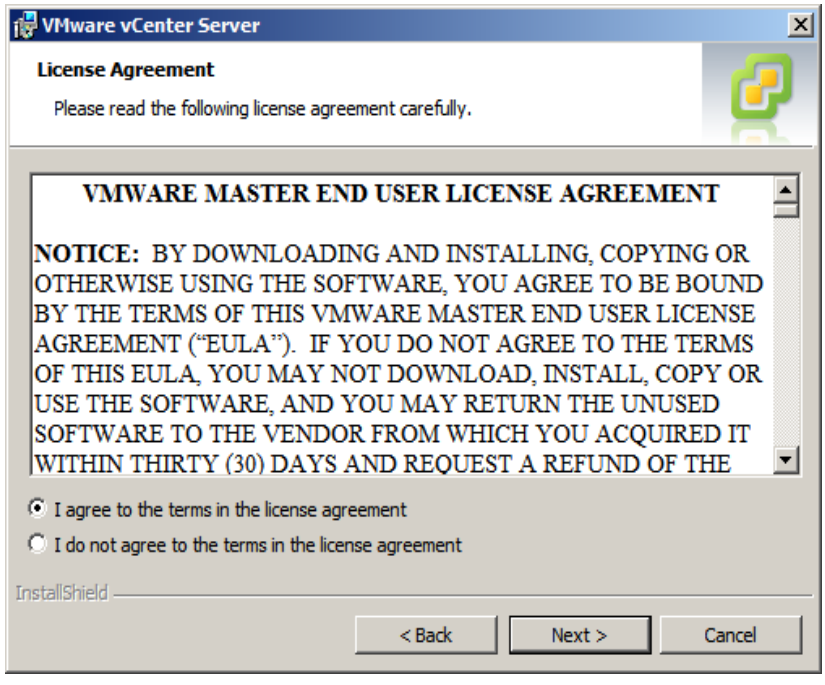
vCenterin 4.1 asennus:

VMware ESX and vCenter Server Installation Guide

Käynnistetään vCenter Server asennus VIM-asennustiedostosta ja valitaan vCenter Server. Valitaan asennettavaksi vCenter Server (kuva 1).

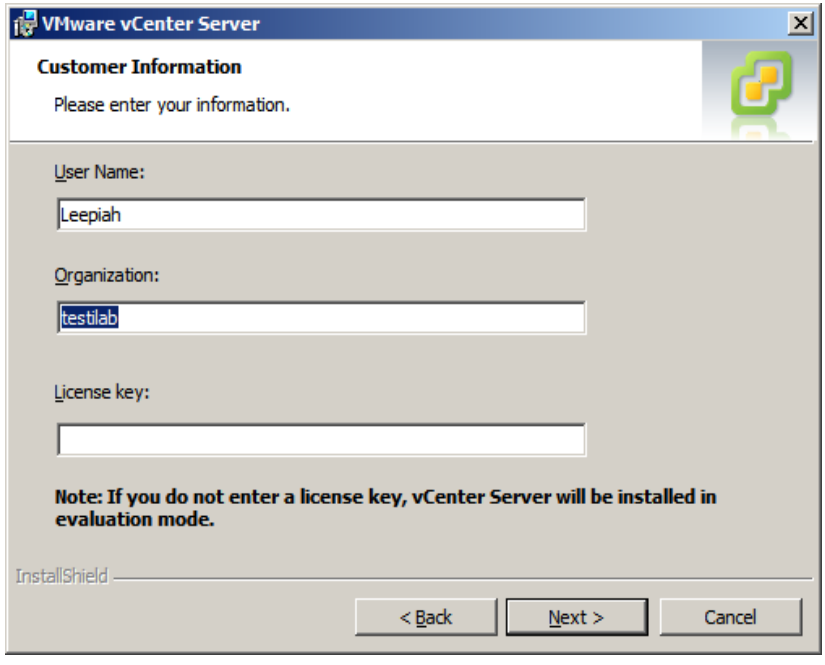
Kuva 1. Valitaan asennettavaksi vCenter Server.

Luetaan ja hyväksytään lisenssiehdot (kuva 2).



Kuva 2. Luetaan ja hyväksytään lisenssiehdot.

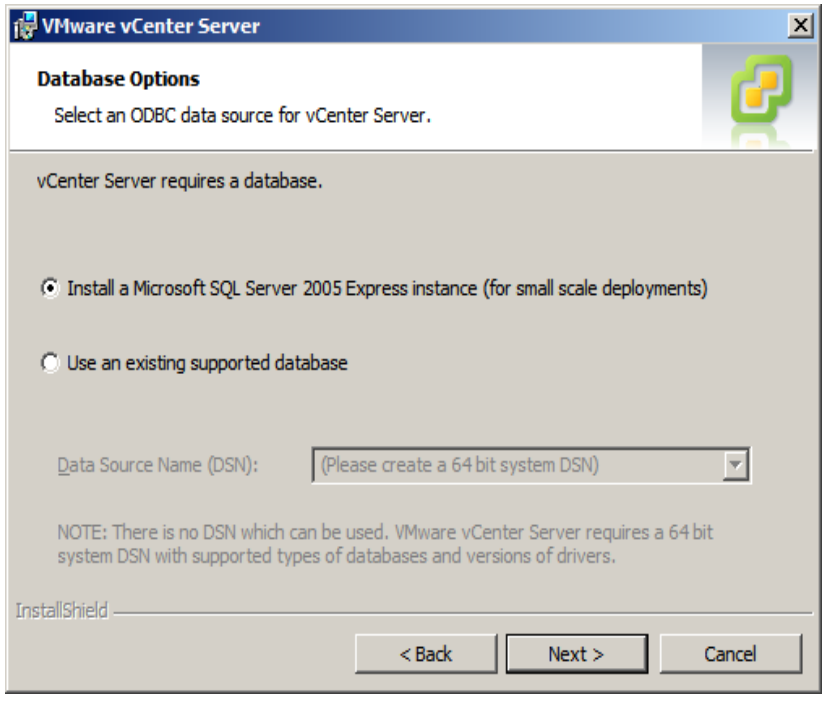
Lisätään käyttäjän ja organisaation tiedot sekä virallinen lisenssiavain (kuva 3). Tässä tapauksessa lisenssiavainta ei tarvitse kirjata, koska kyseessä on testi-versio (60 pv). Painetaan ”Next”.



Kuva 3. Lisätään käyttäjän ja organisaation tiedot sekä virallinen lisenssiavain.

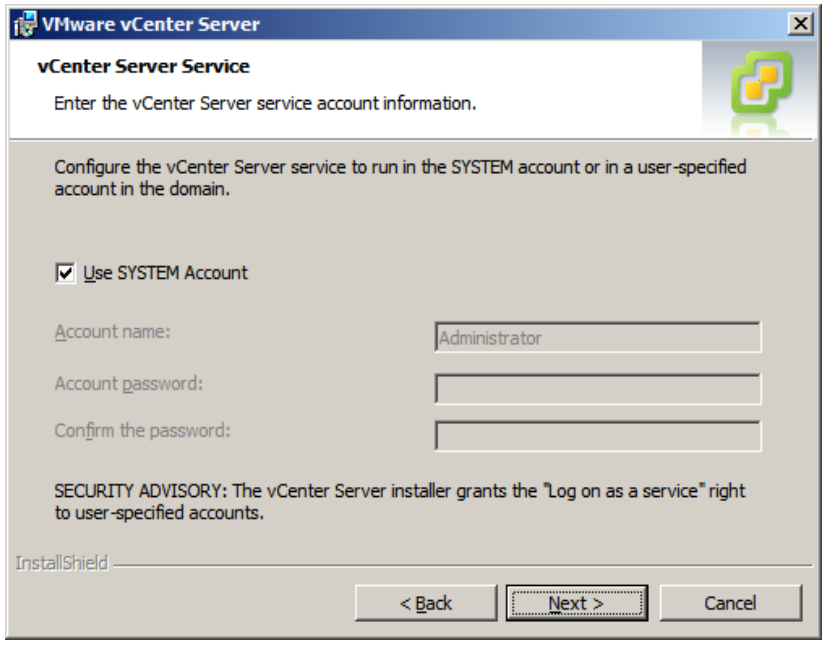
vCenter vaatii tietokantaohjelmiston isäntäkoneiden ja virtuaalikoneiden tietojen varastoimiseen. Jos käytössä on vähemmän kuin viisi isäntäpalvelinta tai vä-

hemmän kuin 50 virtuaalikonetta, sopivaksi tietokantaohjelmistoksi soveltuu Microsoft SQL 2005 Express. Muussa tapauksessa käytetään kehittyneempiä versioita. Testiympäristöön valittiin asennuksen tarjoama versio (kuva 4).



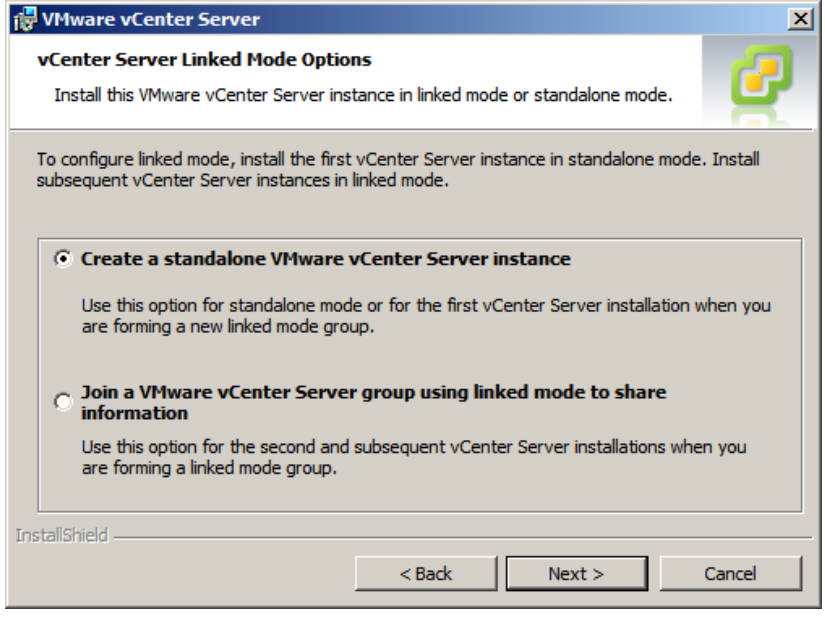
Kuva 4. Valitaan tietokantaohjelmistoksi Microsoft Server 2005 Express

Seuraavaksi määritellään tunnukset vCenterin hallintaan kirjautumiseen. Kirjautumisessa voi käyttää Active Directoryn pääkäyttäjän tunnuksia tai vCenterille voidaan määrittää oma tunnus. Testiympäristössä valitaan käyttöön pääkäyttäjän tunnukset (kuva 5). Tällöin käytännössä vCenterille kirjautuessa käytetään samaa tunnusta, jota käytetään AD-palvelimelle kirjauduttaessa.



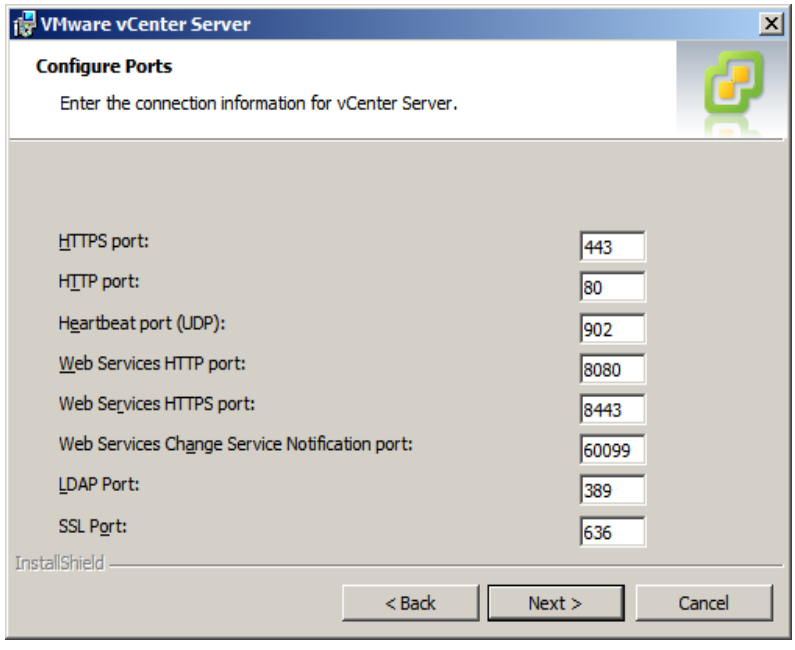
Kuva 5. Kirjautumistapa vCenterille.

Seuraavassa kohdassa valitaan VMware vCenter standalone tai linked mode –asennuksena (kuva 6). Ensimmäiselle vCenter:lle tulee valita standalone. Valitaan kohta “Create a standalone VMware vCenter Server instance”. Jos tarvitaan toinen VMware vCenter Serveri, se asennetaan linked mode -asennuksena.



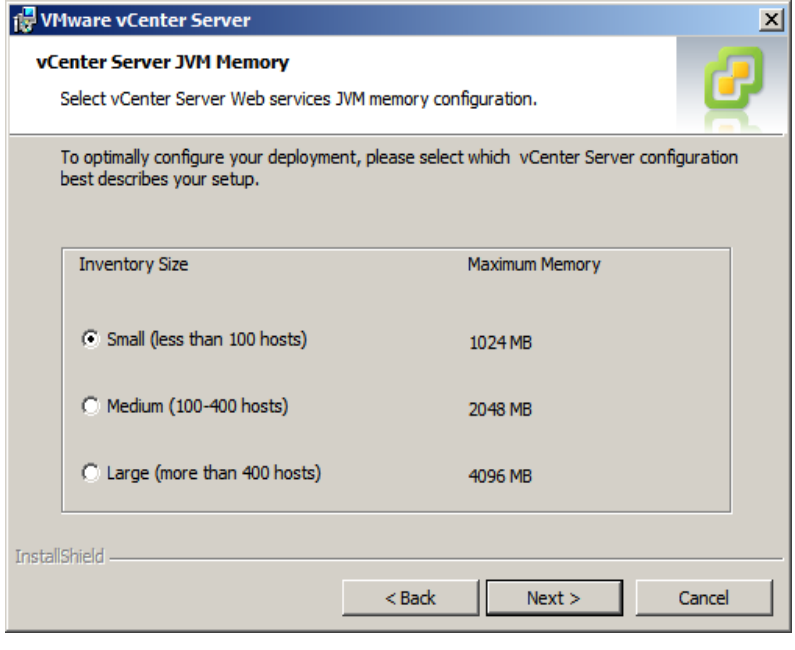
Kuva 6. Luodaan VMware standalone-asennuksena.

Kuvassa 7 määritellään järjestelmässä käytettävien tietoliikenneporttien asetukset. Testiympäristössä porttien asetukset hyväksyttiin oletusasetuksin.

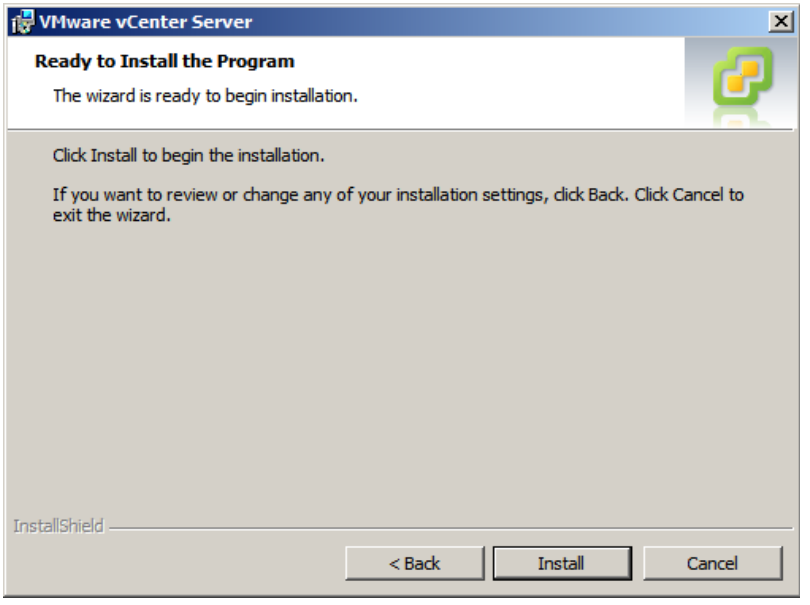


Kuva 7. Järjestelmän tietoliikenneportit

vCenter Server JVM muistinvarauksessa valitaan asetukset View-ympäristössä esiintyvien isäntäpalvelimien lukumäärän mukaan. Testiympäristössä valittiin ”Small” (kuva 8).



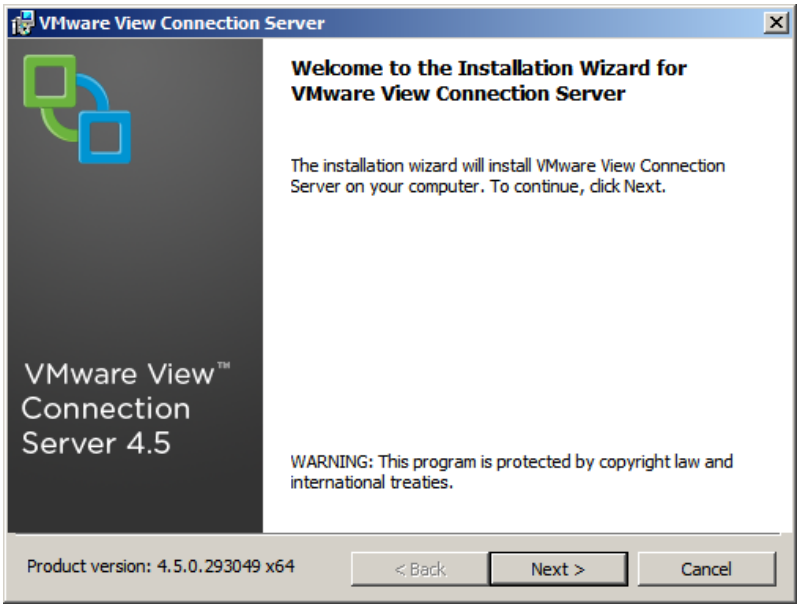
Kuva 8. vCenter muistinvaraus View-ympäristössä toimiville isäntäpalvelimille. Käynnistetään asennus valitsemalla “Install” (kuva 9).



Kuva 9. Aloitetaan asennus painamalla ”Install”.

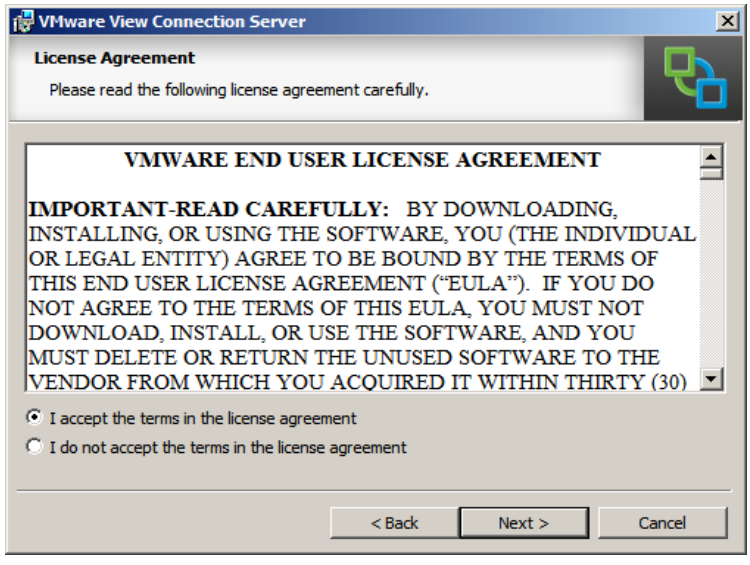
VMware View Connection Server 4:n asennus: VMware View Installation Guide

Käynnistetään VMware Connection Server asennustiedosto (kuva 10).



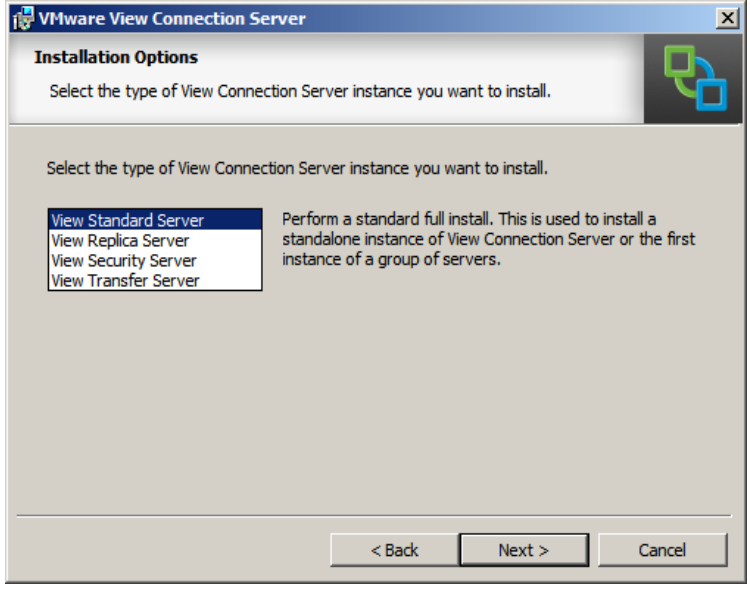
Kuva 10. Aloitetaan View Connection Server -asennus painamalla ”Next”.

Hyväksytään lisenssiehdot (kuva 11).



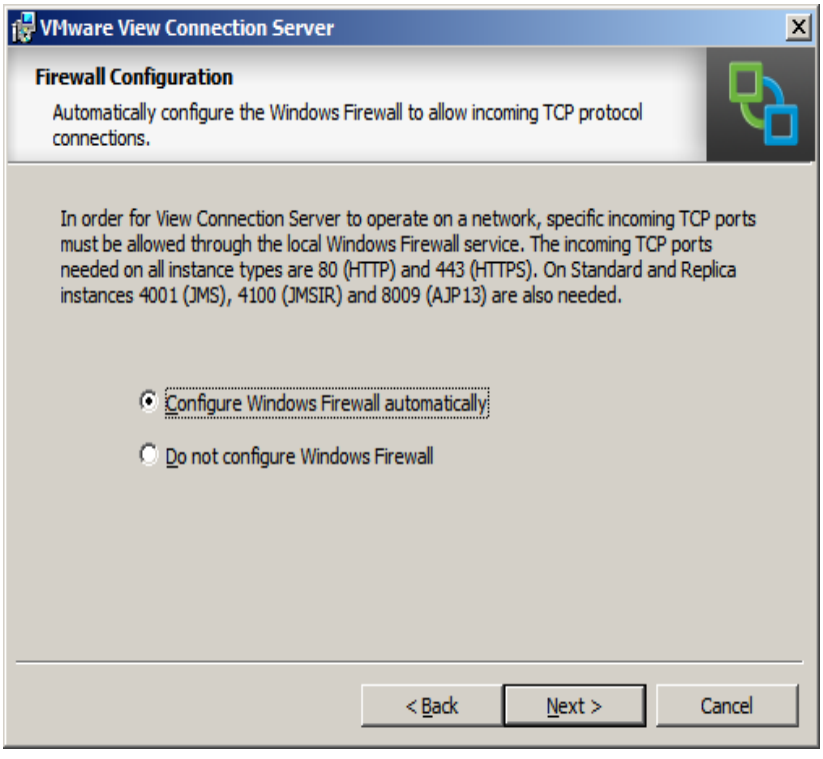
Kuva 11. Hyväksytään lisenssiehdot.

Ensimmäisen Connection Server asennuksen yhteydessä valitaan View Standard Server (kuva 12). Jos ensimmäisen asennuksen lisäksi tarvitaan useampi Connection Server, asennusmääritykseksi valitaan Replica.



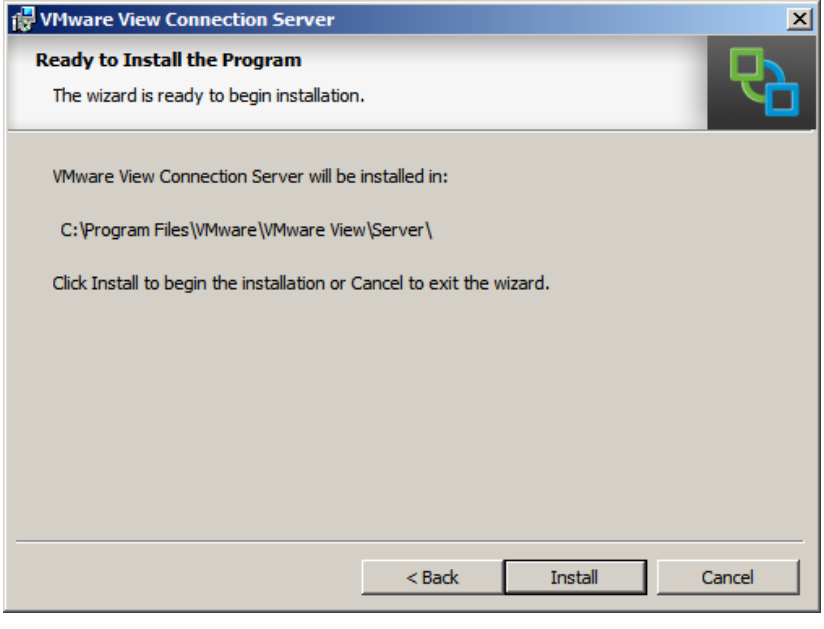
Kuva 12. Asennetaan Connection Server View Standard Server -asennuksena.

Palomuuriasetukset asetetaan automaattisesti tai manuaalisesti. Valitaan automaattinen asetus (kuva 13).



Kuva 13. Palomuurimääritykset.

Käynnistetään asennus painamalla “Install” (kuva 14).

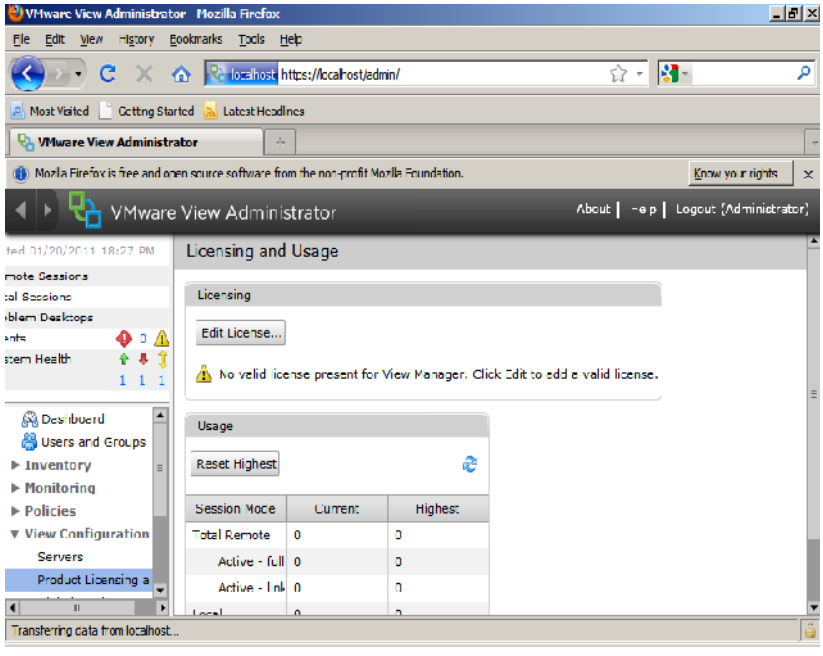


Kuva 14. Käynnistetään asennus painamalla “Install”.

Konfiguroinnit VMware View Administrator's Guide

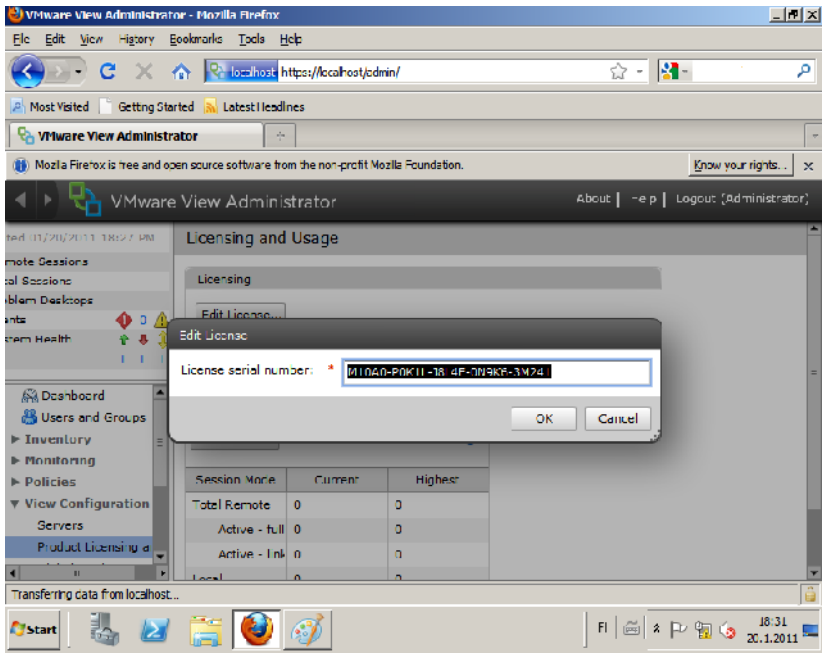
View Connection Serveriä konfiguroidaan ja hallitaan View Administrator web-liittymän kautta kirjoittamalla selaimen osoittekenttään 10.0.0.12 tai https://localhost/admin ja kirjaudutaan sisään toimialueen Administrator -tunnuksilla. Jos käytössä on Explorer -selain, saatetaan tarvita Adobe-lisäosan asennus selaimeen. Tästä syystä työssä asennettiin palvelimelle Firefox-selain.

Ensimmäiseksi aktivoidaan Connection Server lisäämällä siihen lisenssiavain. Lisensointi suoritetaan valitsemalla View Configuration -valikko, josta valitaan “Product Licensing and Usage” (kuva 15).



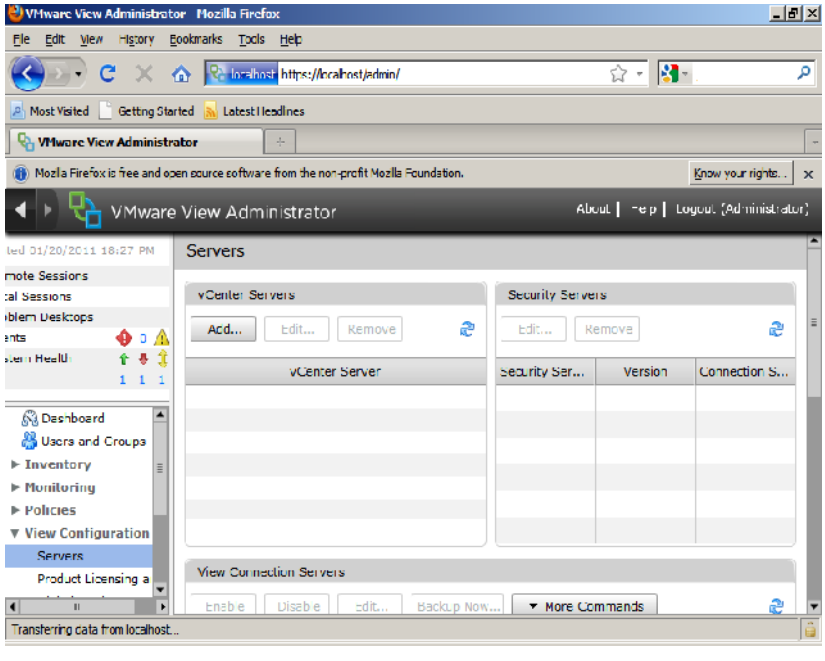
Kuva 15. Connection Serveri lisenssiavaimen lisäys.

Syötetään lisenssiavain ruudussa Edit License (kuva 16).



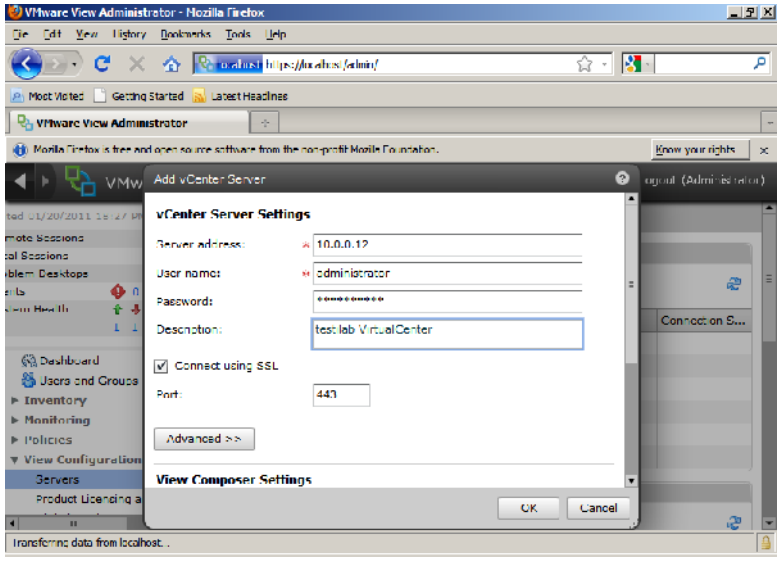
Kuva 16. Connection Serverin lisenssiavain.

Seuraavaksi konfiguroidaan View Manager kytkeytymään vCenter Server -instanssiin. vCenter Serverillä luodaan ja hallitaan virtuaalikoneita, joita View Manager käyttää työpöytälähteenä. Valitaan View Administrator käyttöliittymässä kohta View Configuration → Servers. vCenter Servers paneelin alta valitaan ”Add” (kuva 17).



Kuva 17. vCenter-asetukset.

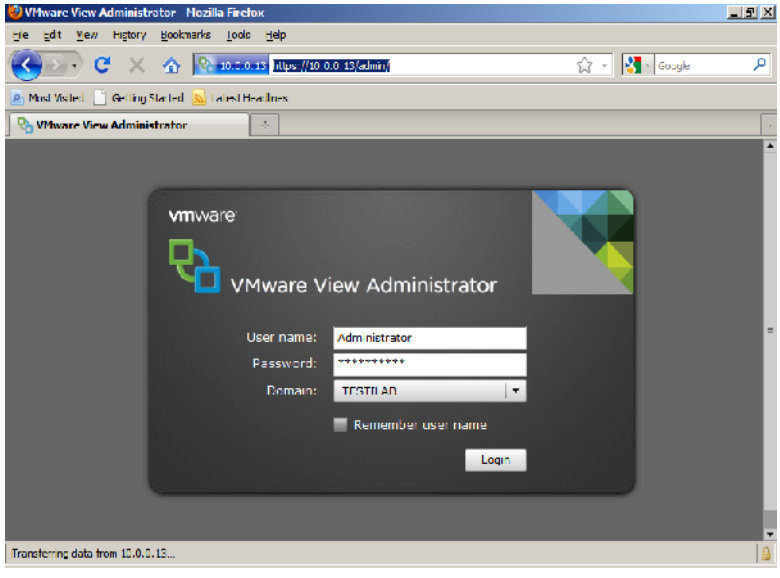
Lisätään vCenter-palvelimen tiedot (kuva 18). Server address -kenttään laitetaan palvelimen IP-osoite tai sen FQDN (fully qualified domain name) Win-vCenter.testilab.local. Domain-tunnukset ja muut asetukset hyväksytään oletuksin. Vahvistetaan asetukset painamalla OK.



Kuva 18. Lisätään vCenter-palvelimen tiedot.

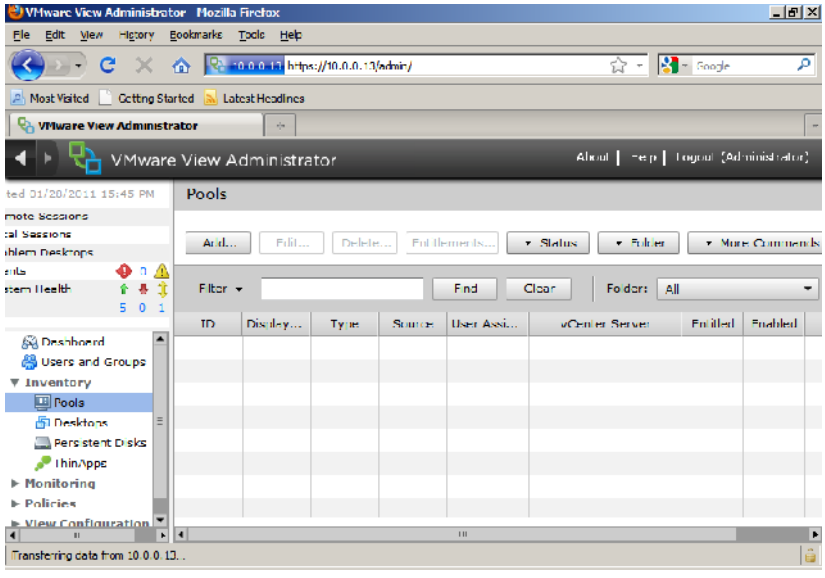
ADD VIRTUAL DESKTOP POOL

VMware Connection -palvelimen selaimella mennään osoitteeseen 10.0.0.13. Kirjaudutaan käyttöliittymässä Administrator-tunnuksilla sisään (kuva 19).



Kuva 19. Kirjaudutaan VMware View Administrator -käyttöliittymään.

Käynnistetään Desktop poolin asennus Inventorin alta Pools--> Add (kuva 20).

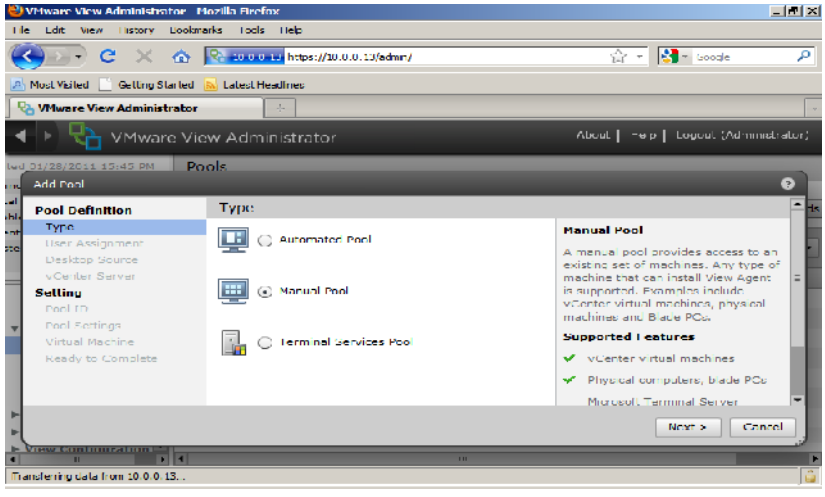


Kuva 20. Käynnistetään Desktop poolin asennus Inventorin alta Pools ja Add.

Desktop polityypiksi voidaan valita Automated Pool, Manual Pool tai Terminal Services Pool (kuva 21):

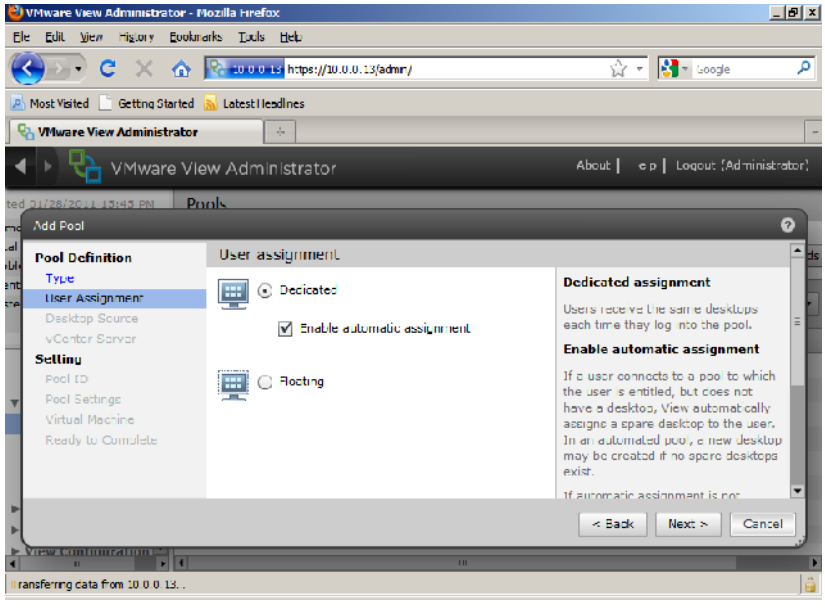
- Automated Desktop Pool sisältää yhden tai useamman dynaamisesti luodun työpöydän, joka on automaattisesti luotu ja määritelty View Managerissa ja poimittu vCenterillä sijaitsevasta virtuaalikoneen mallitiedostosta (template). Automaattinen pooli voidaan määrittää pysyvänä (persistent) tai ei-pysyvänä (non-persistent) työasemavarantona. Pysyvässä vaihtoehdossa käyttäjälle annetaan käyttöön työpöytä, joka sisältää käyttäjän asetukset, dokumentit ja tarvittavat sovellukset. Ei-pysyvässä vaihtoehdossa työpöytiin liitetyt sovellukset pysyvät tallessa vain istunnon ajan. Istunnon jälkeen tiedot hävitetään.

- Manual Desktop Pool luodaan olemassa olevista virtuaalikoneista (vCenterin hallinnassa), fyysisistä PC-koneista tai Blade PC-koneista. View-järjestelmään kirjauduttaessassa tietokonevarannosta otetaan käyttöön haluttu työasema.
- Terminal Services Poolilta eli Microsoftin terminaalipalvelimelta voidaan järjestää terminaalipohjainen työpöytäyhteys View:n käyttäjille.
- Testiympäristössä otettiin käyttöön Manual Pool.



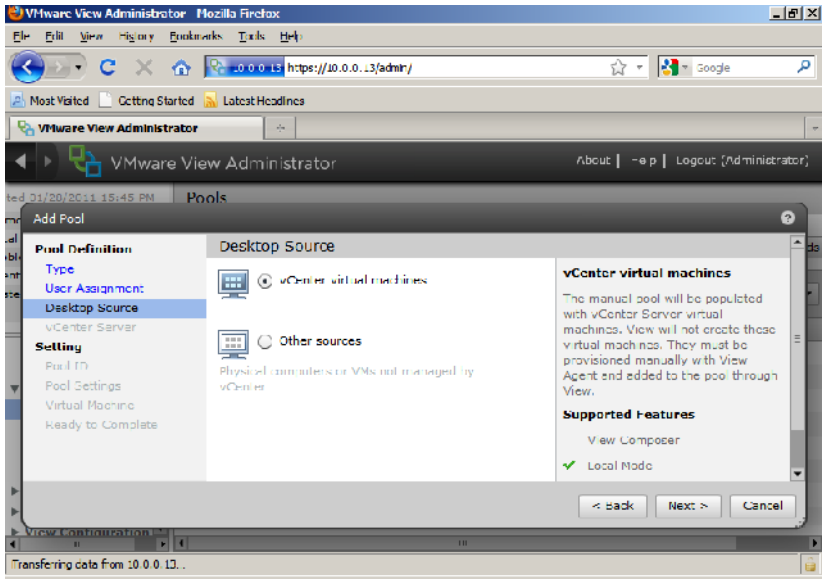
Kuva 21. Valitaan poolityyppi.

Käyttäjän nimeäminen työpöydälle dedicated tai floating -asetuksella. Dedicated valitaan, jos käyttäjälle halutaan nimetä henkilökohtainen työpöytä. Floating-valinnalla työpöytä on käytettävissä kaikille pooliin lisätyille käyttäjille. Testiympäristössä valittiin dedicated-asetus (kuva 22).



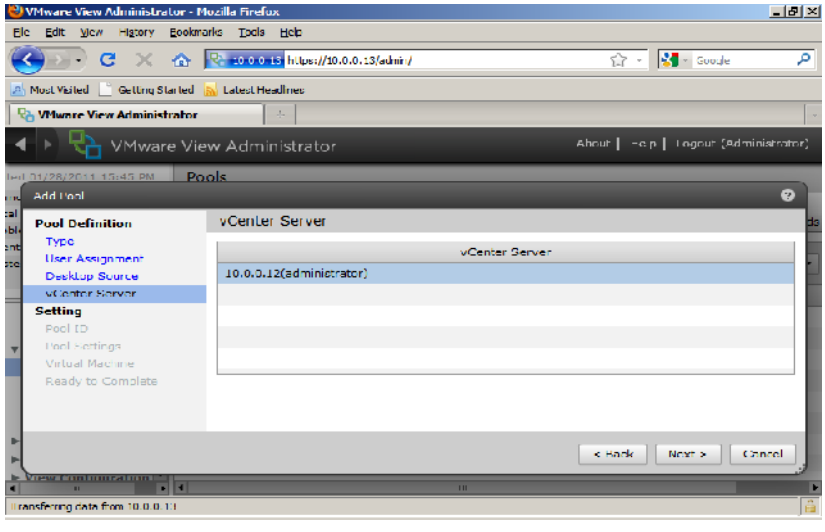
Kuva 22. Käyttäjän nimeäminen työpöydälle dedicated tai floating asetuksella.

Seuraavaksi valitaan työpöytälähde, josta virtuaalikone poimitaan pooliin (kuva 23). Työpöytälähteenä on vCenter tai jokin muu. Työpöytälähteeksi valitaan vCenter.



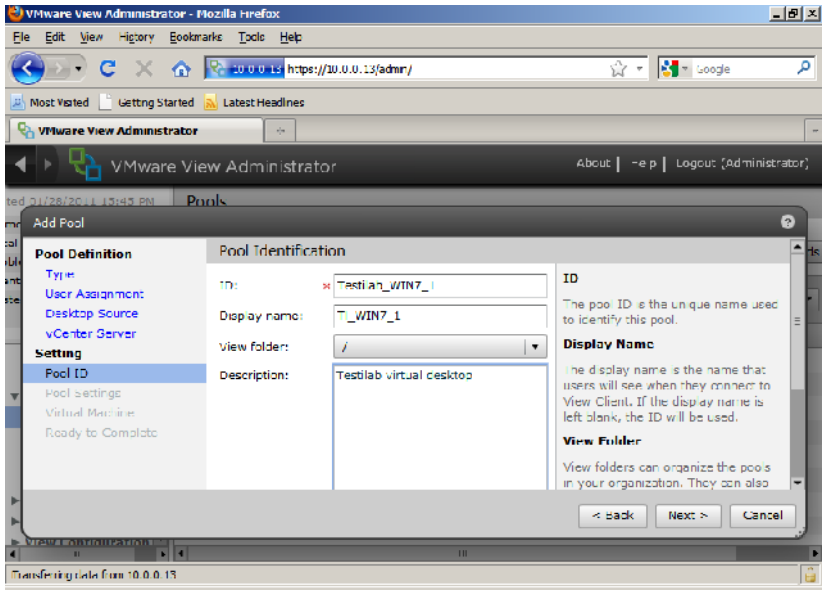
Kuva 23. Valitaan työpöytälähde, josta virtuaalikone poimitaan pooliin.

Seuraavassa vaiheessa näytetään vCenter palvelimen IP-osoite (kuva 24).



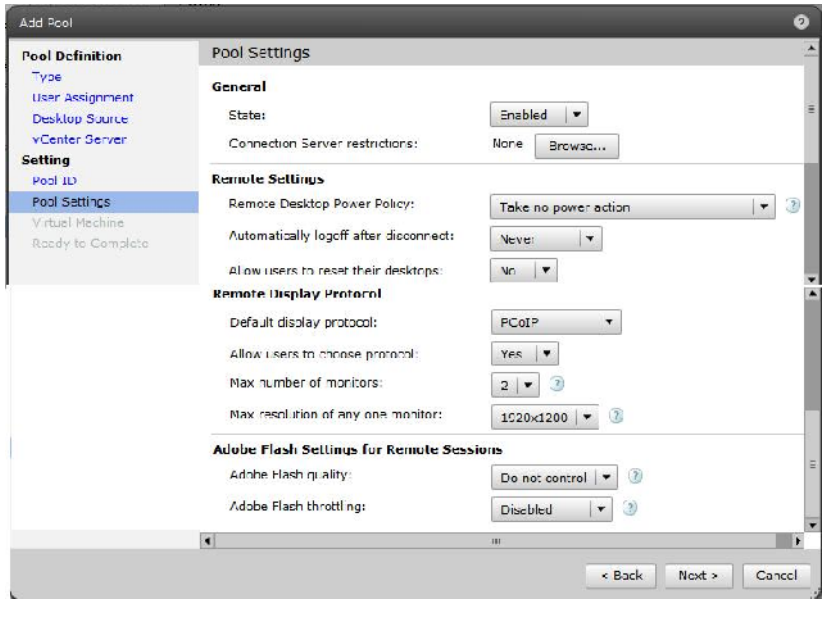
Kuva 24. vCenterin IP-osoite.

Pool identification -kohdassa määritellään poolille ID-tunnus (pakollinen), Display name ja Description. Display name -kenttään lisätty nimi näkyy View-asiakkaalle (kuva 25). Description-kenttään voidaan lisätä kuvaus poolista.



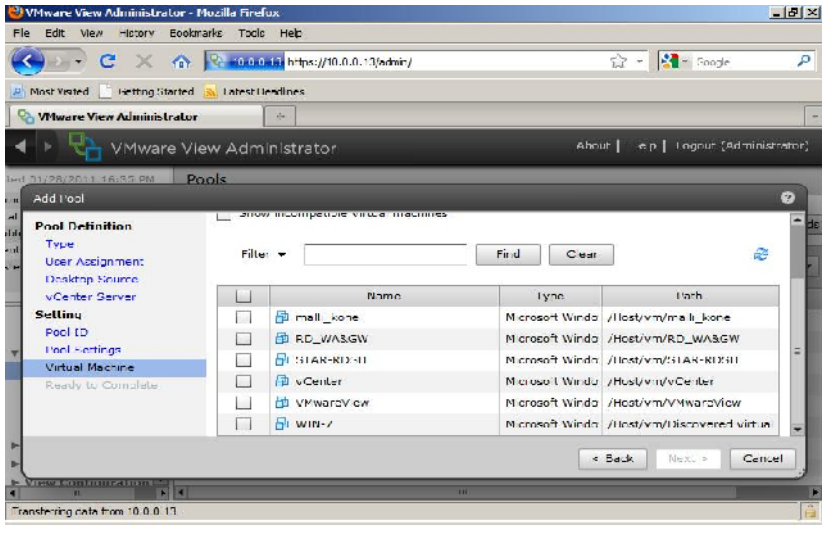
Kuva 25. Poolin tiedot.

Pool Settings -kohdassa voidaan tehdä seuraavia määrityksiä: Yhteysasetukset, työpöydän etäkäyttöprotokolla,näyttöjen määrä, näyttöjen resoluutio ja flash-laatumääritykset (kuva 26).



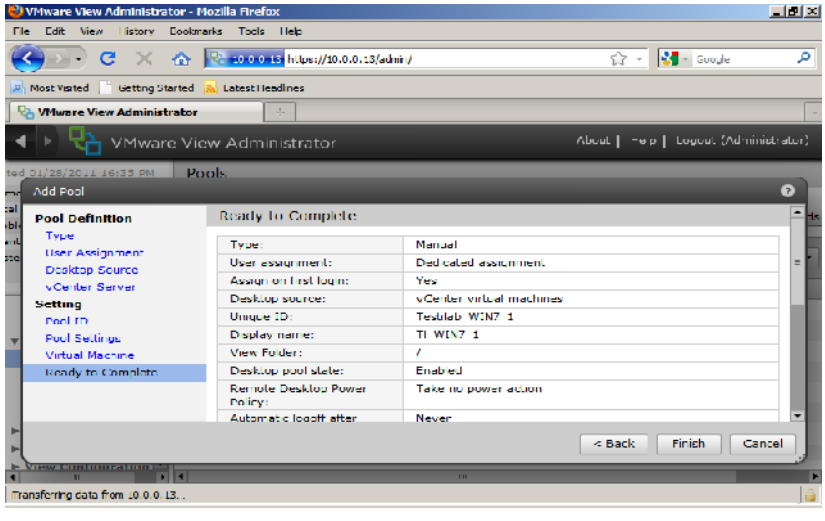
Kuva 26. Poolin asetukset.

Tässä kohdassa valitaan ne työpöydät, jotka lisätään pooliin (kuva 27). Pooliin lisättiin listalta WIN-7 virtuaalikone Windows 7 -käyttöjärjestelmällä.



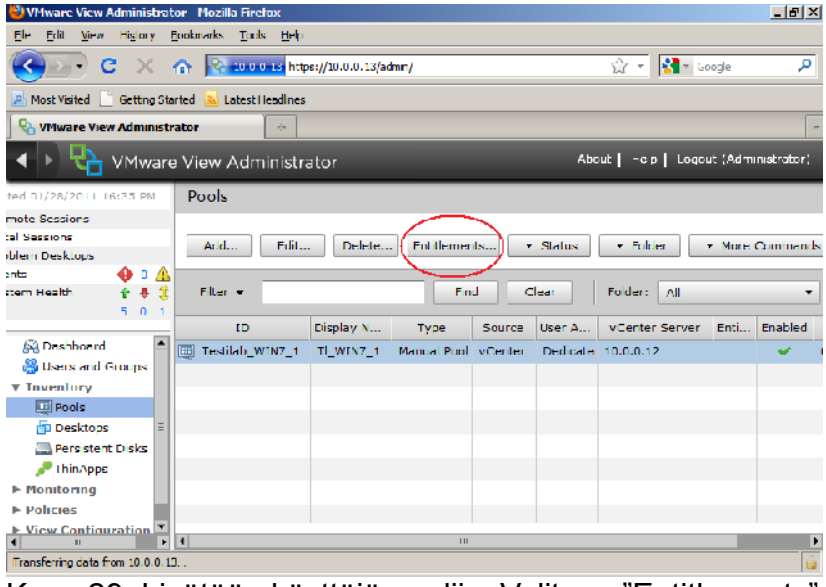
Kuva 27. Valitaan ne työpöydät, jotka lisätään pooliin.

Poolimääritysten lopussa tulee näkyville yhteenveto tehdyistä asetuksista (kuva 28).



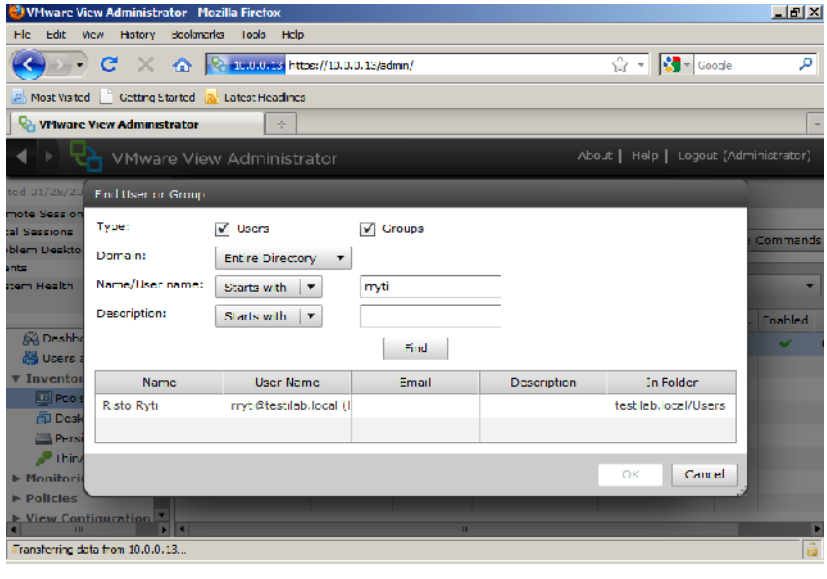
Kuva 28. Yhteenveto poolimäärityksistä.

Poolin luomisen jälkeen nimetään pooliin käyttäjä (29). Käyttäjän lisääminen poolin tehdään valitsemalla ”Inventoryn” alta ”Pools” ja klikataan kohtaa ”Entitlements”.



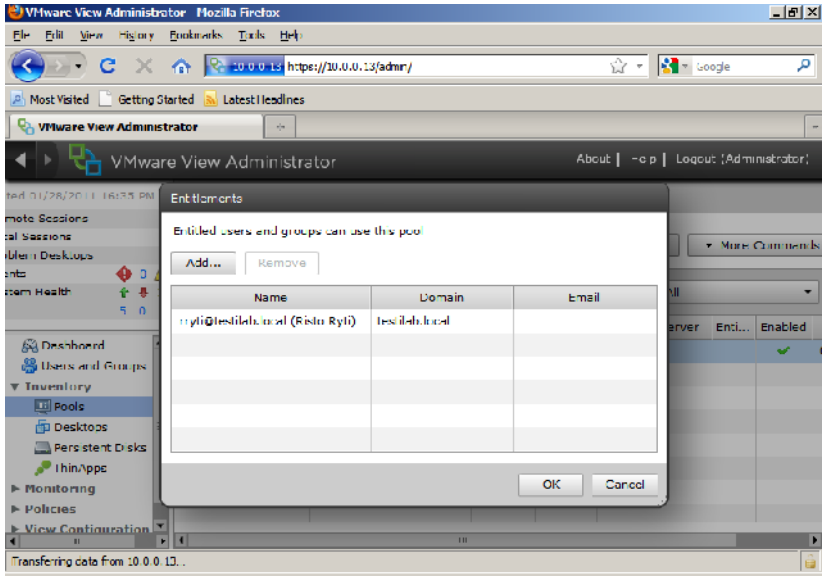
Kuva 29. Lisätään käyttäjä pooliin. Valitaan ”Entitlements”.

Seuraavassa kohdassa on mahdollista lisätä pooliin halutut käyttäjät tai ryhmät (kuva 30). Syötetään käyttäjän tai ryhmän tiedot seuraaviin kenttiin: Domain, käyttäjän nimi ja kuvaus käyttäjästä. Listalle tuli automaattisesti esille toimialueen käyttäjä Risto Ryti, joka valittiin poolin WIN-7 koneen käyttäjäksi.



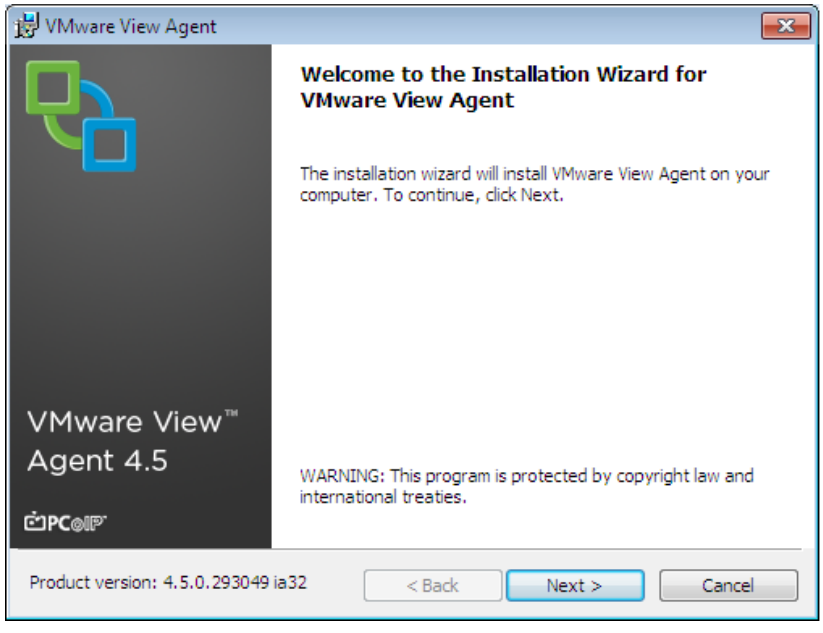
Kuva 30. Lisätään haluttu käyttäjä pooliin.

Lopuksi listalle tulee näkyviin pooliin lisätty käyttäjä Risto Ryti ja valitaan käyttäjä painamalla ”OK” (kuva 31).



Kuva 31. Lisätty käyttäjä näkyy ruudulla.

Asennetaan VMware View Agent -palvelu vCenterin hallinnoimaan WIN-7-virtuaalikoneeseen, jotta View Connection Server voi kommunikoida niiden kanssa. Käynnistetään View Agent asennus ja painetaan ”Next” (kuva 32).

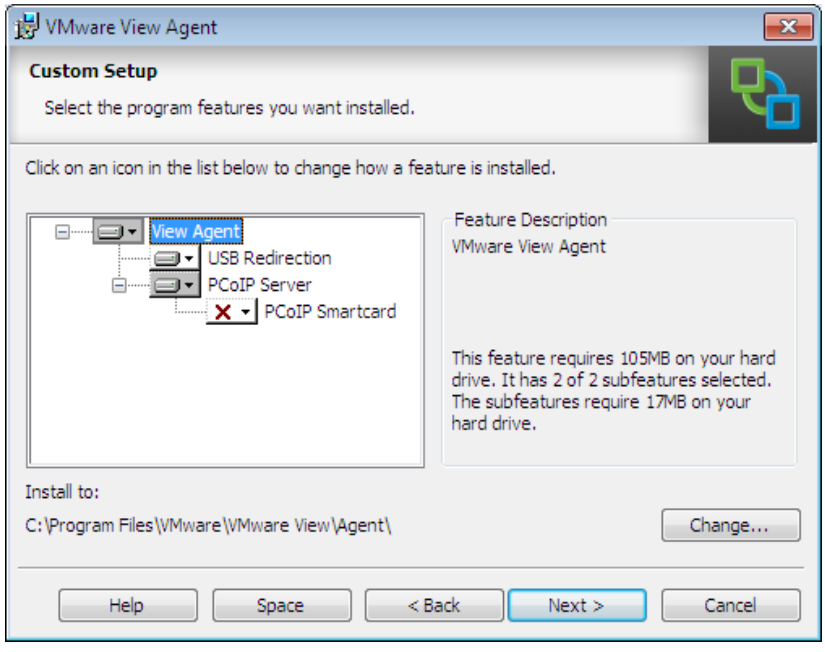


Kuva 32. Käynnistetään View Agent asennus ja painetaan ”Next”.

Luetaan ja hyväksytään lisenssiehdot, painetaan ”Next” (kuva 33).

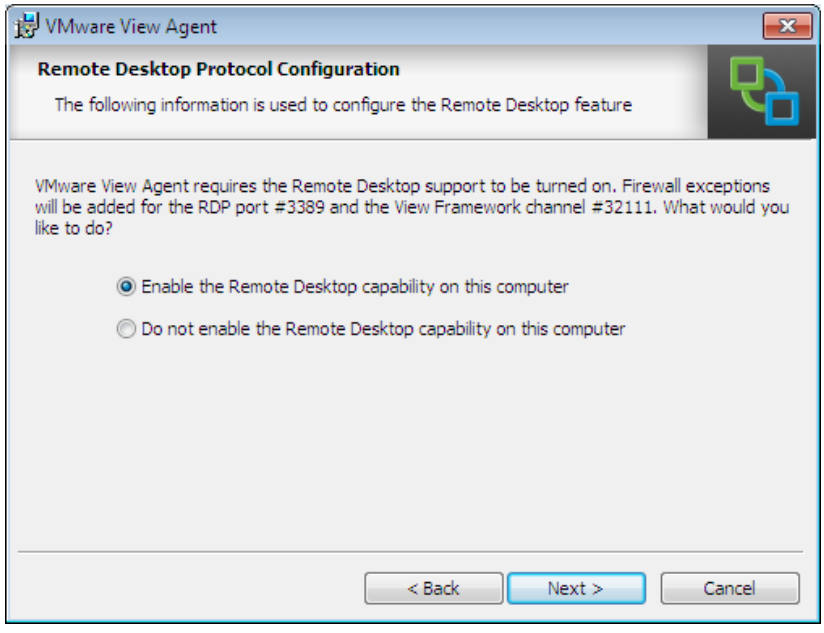
Kuva 33. Luetaan ja hyväksytään lisenssiehdot, painetaan ”Next”.

Valitaan View Agent -komponentit (kuva 34). Opinnäytetyössä asetukset hyväksyttiin oletusasetuksin; tuki USB:lle ja PcoIP Server jätettiin valitsematta, koska testiympäristössä ei ollut käytössä älykorttia.



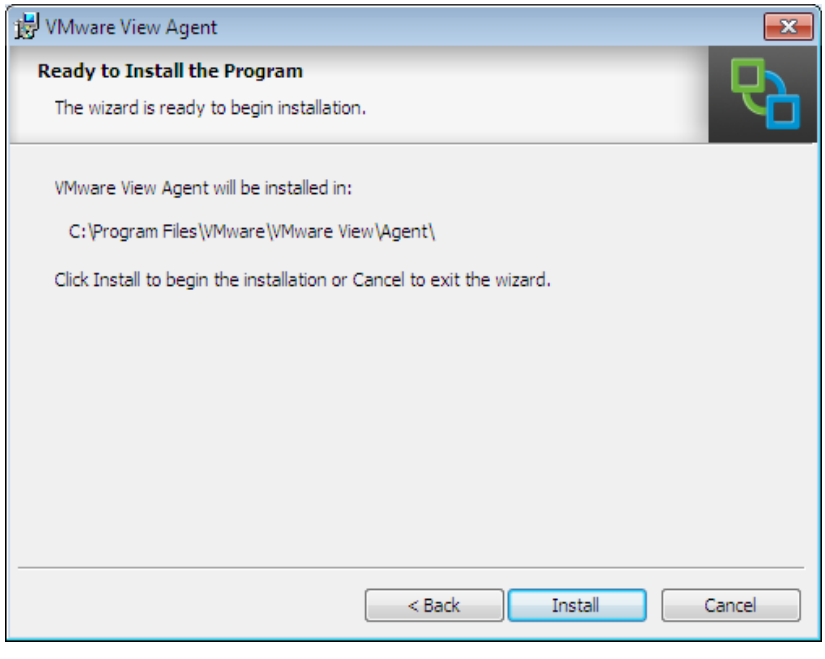
Kuva 34. Valitaan View Agent -komponentit.

Etätyöpöytäprotokollan konfiguraatiossa sallitaan etätyöpöydän käyttö (kuva 35).



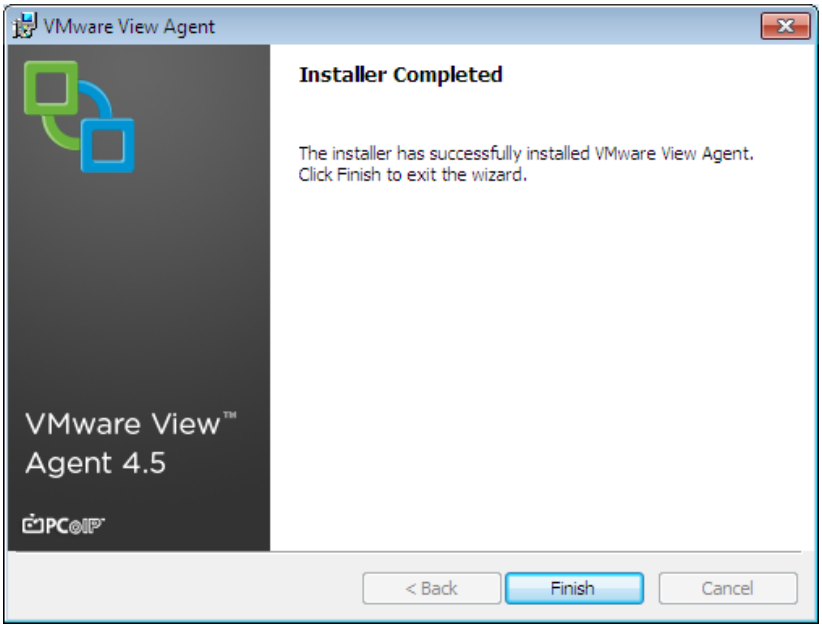
Kuva 35. Sallitaan etätyöpöydän käyttö.

Ruudulle tulee näkyviin asennuksen sijainti. Aloitetaan asennus painamalla, ”Install” (kuva 36).



Kuva 36. Aloitetaan asennus painamalla, ”Install”.

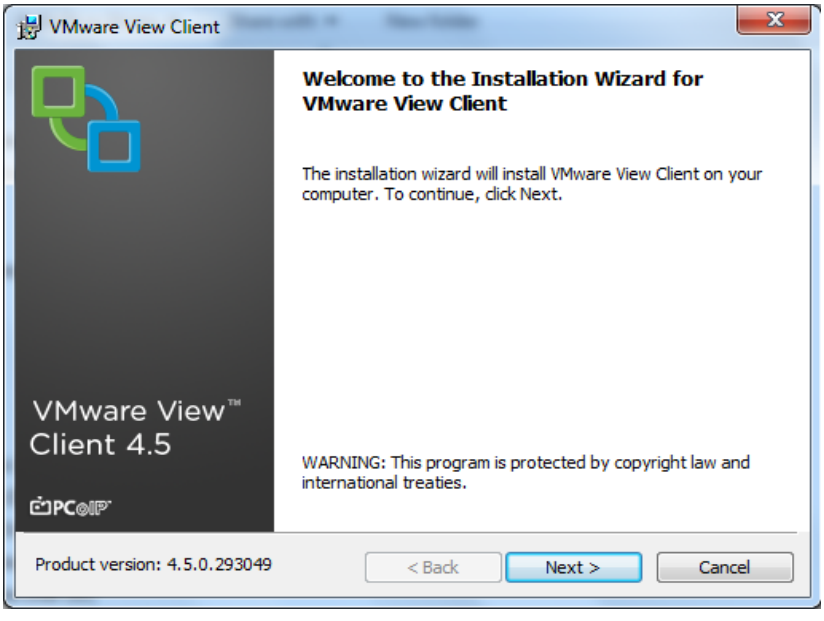
Asennuksen päätteeksi painetaan ”Finish” (kuva 37).



Kuva 37. Asennuksen päätteeksi painetaan ”Finish”.

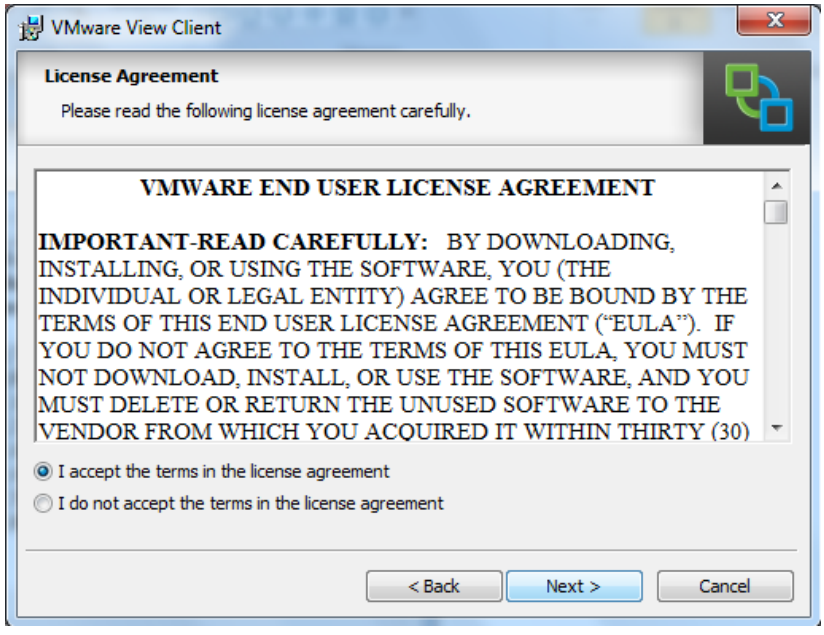
Asennetaan client:

Käynnistetään VMware View Client 4.5 -asennus (32- tai 64-bit) asennustiedostosta ja painetaan ”Next” (kuva 38).



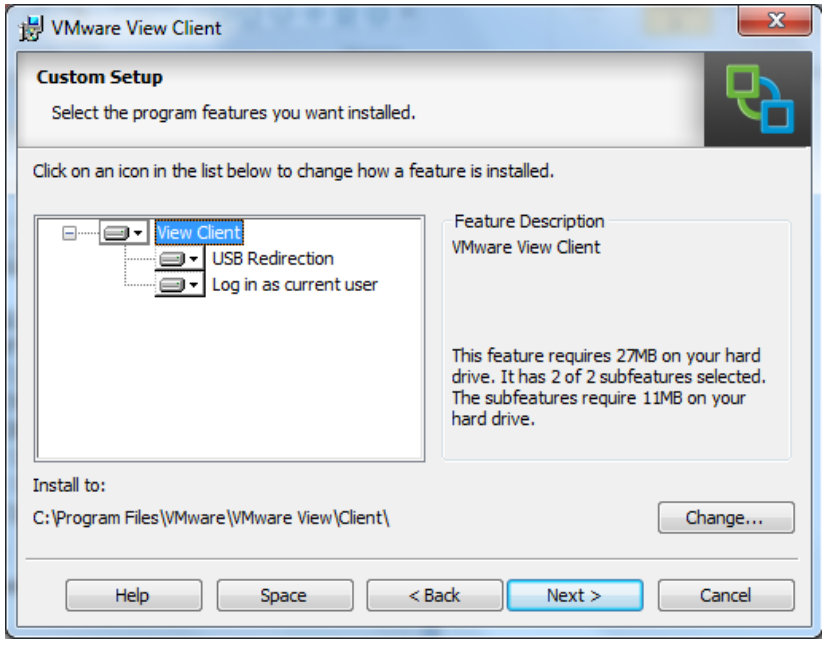
Kuva 38. Aloitetaan View-clientin asennus painamalla ”Next”.

Luetaan ja hyväksytään lisenssiehdot (kuva 39).



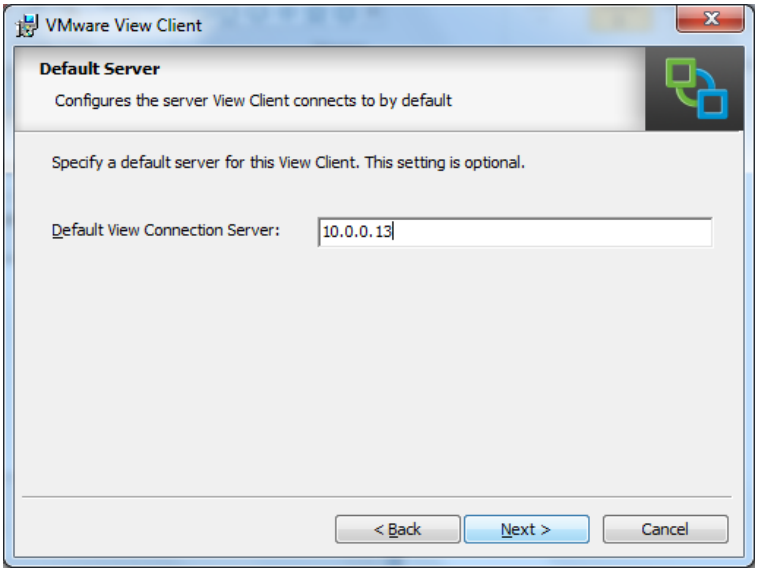
Kuva 39 Luetaan ja hyväksytään lisenssiehdot.

Valitaan View Client -komponentit. Asetukset hyväksytään oletuksin ja painetaan ”Next” (kuva 40).



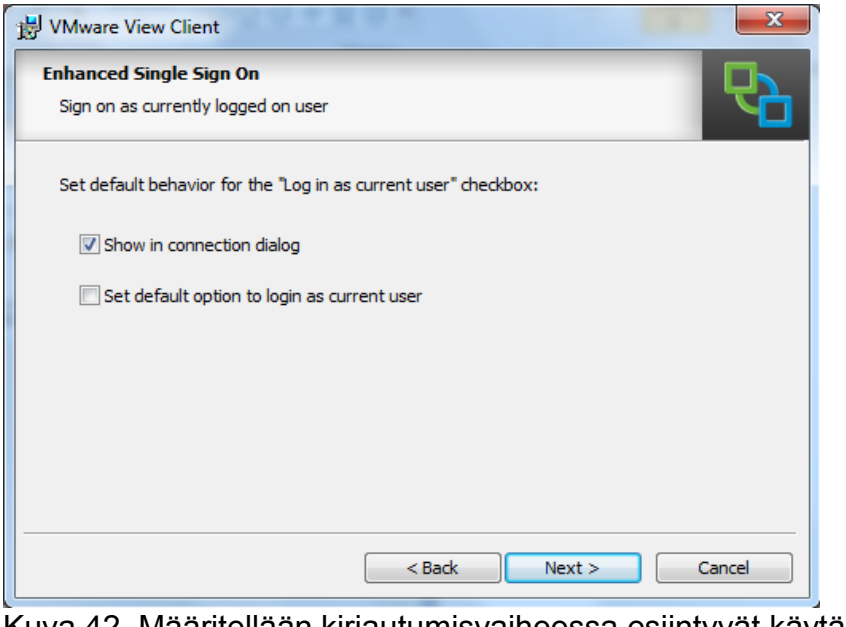
Kuva 40. Valitaan View Client -komponentit.

Konfiguroidaan View Clientille oletus View Connection Server (kuva 41). Lisätään testiympäristön View Connection Serverin IP-osoite: 10.0.0.13. Tämä asetus on valinnainen.



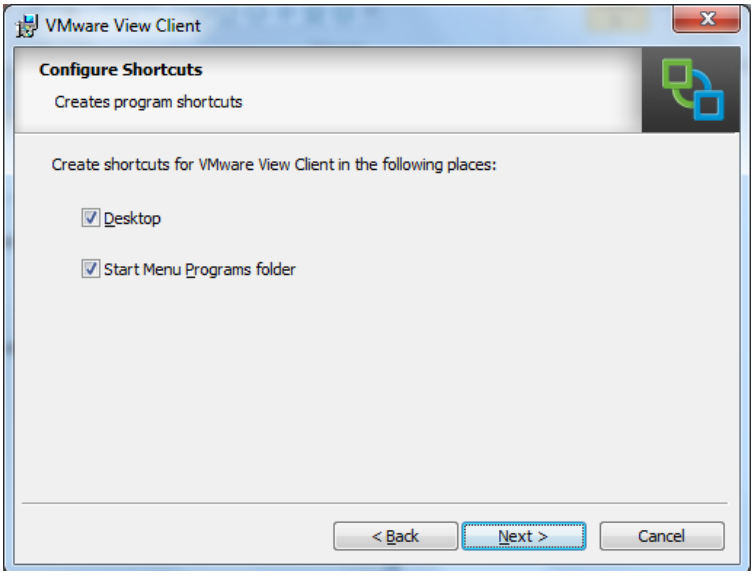
Kuva 41. Lisätään View Connection Serverin IP-osoite.

Määritellään kirjautumisvaiheessa esiintyvät käytännöt (kuva 42).



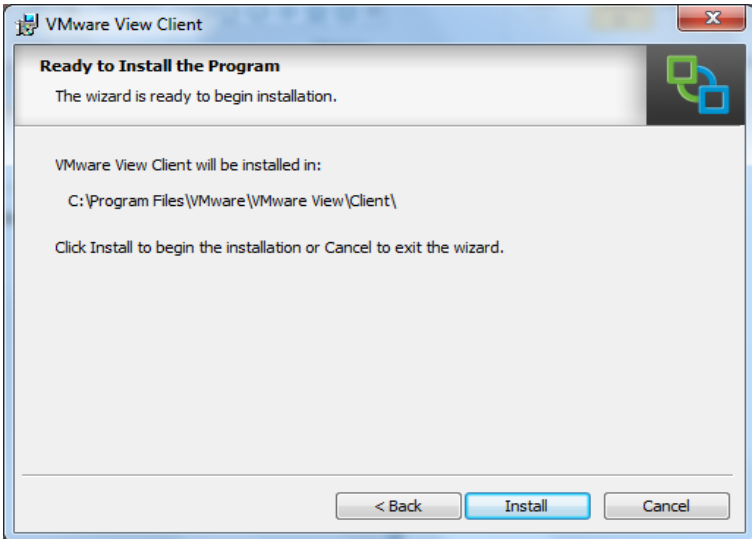
Kuva 42. Määritellään kirjautumisvaiheessa esiintyvät käytännöt.

View Client -pikakuvake voidaan valita näkymään työpöydällä tai käynnistä-valikossa (kuva 43).



Kuva 43. View Client -pikakuvake voidaan valita näkymään työpöydällä tai käynnistä-valikossa.

Lopuksi näytetään View Client -asennuksen sijainti kovalevyllä ja painetaan asennuksen käynnistämiseksi ”Install” (kuva 44).



Kuva 44. Painetaan asennuksen käynnistämiseksi ”Install”.

Reitittimen konfiguraatio:

```
show ru
*Jan 11 18:27:47.703: %CDP-4-DUPLEX_MISMATCH: duplex mismatch dis-
covered on FastEthernet0/1.1 (not half duplex), with Switch FastEthernet0/1
(half duplex).
ISP#show run
Building configuration...

Current configuration : 1392 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$OBxm$MnXHfb9cKRPGR.ztx3dcO.
!
no aaa new-model
!
resource policy
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
 --More--ip subnet-zero
ip cef
!
!
no ip dhcp use vrf connected
!
!
no ip domain lookup
!
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 speed 100
 full-duplex
!
```

```
 --More--interface FastEthernet0/1.1
 description Management VLAN 1
 encapsulation dot1Q 1 native
 ip address 192.168.1.1 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.10
 description RDS VLAN 10
 encapsulation dot1Q 10
 ip address 192.168.0.1 255.255.255.0
 no snmp trap link-status
!
interface FastEthernet0/1.20
 description ExternalN VLAN 20
 encapsulation dot1Q 20
 ip address 192.168.2.1 255.255.255.0
 no snmp trap link-status
!
interface Serial0/0/0
 no ip address
 shutdown
 clockrate 125000
!
 --More--interface Serial0/0/1
 no ip address
 shutdown
 clockrate 125000
!
router eigrp 10
 network 192.168.0.0
 network 192.168.1.0
 network 192.168.2.0
 no auto-summary
!
ip classless
!
ip http server
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
 --More--line vty 0 4
 login
!
end
ISP#
```

Kytkimen konfiguraatio:

```
show run
Building configuration...

Current configuration : 1998 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
enable secret 5 $1$vKPP$d88BaggV7MELdxOC3S0hG/
!
ip subnet-zero
!
no ip domain-lookup
!
no file verify auto
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
 --More--!
!
interface FastEthernet0/1
 description Trunk Link to ISP Router
 switchport mode trunk
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet0/6
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet0/7
 switchport access vlan 10
 spanning-tree portfast
 --More--!
```

```
interface FastEthernet0/8
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet0/9
 switchport access vlan 10
 spanning-tree portfast
!
interface FastEthernet0/10
!
interface FastEthernet0/11
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/12
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/13
 switchport access vlan 20
 spanning-tree portfast
!
 --More--interface FastEthernet0/14
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/15
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/16
 switchport access vlan 20
 spanning-tree portfast
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
 --More--!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
```

```
 switchport mode trunk
!
interface GigabitEthernet0/2
 switchport mode trunk
!
interface Vlan1
 ip address 192.168.1.2 255.255.255.0
 no ip route-cache
!
ip default-gateway 192.168.1.1
ip http server
!
line con 0
 exec-timeout 0 0
 logging synchronous
line vty 0 4
 login
 --More--line vty 5 15
 login
!
!
end

Switch#
```